ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Сборник научных трудов
Всероссийского круглого стола
15 февраля 2018 г.

Московский университет
МВД России имени В.Я. Кикотя, 2018

ISBN 978-5-9694-0609-4

Москва
2018

ББК67.00; 32.973.26
А43

Рецензенты:

– заместитель начальника НЦБ Интерпола МВД России полковник полиции ***С. Н. Бородин***;

– преподаватель кафедры специальной связи в ОВД МВД России кандидат технических наук ***А. В. Рой***.

Редакционный совет:

А. В. Пузарин – председатель;
Д. Н. Захаров – заместитель председателя.

Актуальные проблемы обеспечения кибербезопасности : сборник научных трудов Всероссийского круглого стола. – М. : Московский университет МВД России имени В.Я. Кикотя, 2018. – 404 с.

ISBN 978-5-9694-0609-4

В сборник вошли статьи курсантов, молодых ученых и преподавателей, специализирующихся в сфере обеспечения кибербезопасности Российской Федерации. В них отражены проблемные вопросы контроля и правового регулирования безопасности государства, анализа угроз обеспечения кибербезопасности страны, а также противодействия преступности в сфере информационных технологий.

ББК67.00; 32.973.26

НАУЧНОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ

Усл.-печ. л. 23,50.

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http: //www.mosu.mvd.ru, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Раздел 1. УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ 9

А. С. Овчинский
КРИМИНАЛЬНАЯ СРЕДА ЦИФРОВОГО МИРА КАК ИСТОЧНИК УГРОЗ КИБЕРБЕЗОПАСНОСТИ 9

Е. Н. Яковец, С. Ю. Окилов, Г. Г. Саркисян
ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ 15

Ю. И. Синещук
СИСТЕМОЛОГИЧЕСКИЙ АНАЛИЗ БАЗОВЫХ ПОНЯТИЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ 26

Д. Н. Шурухнова
ОПЫТ ЕВРОПОЛА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 29

В. Г. Бурлов
МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ ВОЙНЫ 33

А. В. Долбилов
КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 38

С. И. Козьминых
ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРРОРИЗМУ 41

Д. В. Милютин, Д. А. Панин
СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА: УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЛИ НОВЫЙ ЭТАП В РАЗВИТИИ ВЫСОКИХ ТЕХНОЛОГИЙ 49

А. В. Долбилов, О. С. Дудко
ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ КИБЕРАТАК НА БАНКИ 56

Н. Ю. Ромашкина, А. В. Долбилов
КИБЕРПРЕСТУПНОСТЬ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ 59

Д. Н. Захаров
УГРОЗЫ СОВРЕМЕННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 62

А. А. Крылов
МОНИТОРИНГ УГРОЗООБРАЗУЮЩИХ ФАКТОРОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ 69

Е. А. Рудых, А. В. Долбилов
МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ 73

Ю. С. Крылова, А. В. Долбилов
РОБЛЕМЫ И РИСКИ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ 76

Е. А. Русскевич
НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ (ст. 274[1] УК): ДОСТОИНСТВА И НЕДОСТАТКИ КРИМИНАЛИЗАЦИИ 81

К. В. Давыдов, М. Б. Кавешников
ТЕРРОРИСТИЧЕСКАЯ УГРОЗА И БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ 86

Раздел 2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В УСЛОВИЯХ КИБЕРУГРОЗ 91

М. А. Репко, К. К. Борзунов
ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ И ЕЕ РЕШЕНИЕ 91

А. Л. Суворов, В. И. Лустин
ЭТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ 97

И. Р. Косачева, А. В. Пузарин
ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ СОВМЕСТНО С ИННОВАЦИОННЫМИ ТЕХНОЛОГИЯМИ ЭНЕРГОСНАБЖЕНИЯ 101

Н. С. Попов, А. В. Пузарин
ТЕХНОЛОГИЯ SOC (SECURITY OPERATIONS CENTER) В СИСТЕМЕ ОВД 107

Б. И. Юдаков, А. В. Пузарин
ЦЕНТР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ (SECURITY OPERATIONS CENTER) 114

С. Н. Золотарев, Д. Н. Захаров
ЗАЩИТА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛАМ СВЯЗИ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ 117

М. И. Титова, Е. Н. Клочкова
ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ ИСОД МВД РОССИИ 121

О. В. Симаков, В. В. Щерба
МАТЕМАТИЧЕСКАЯ ОБФУСКАЦИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ПРОГРАММНОГО КОДА 124

Д. И. Якушев
ПОСЛЕДСТВИЯ «ЛОЖНОЙ ТРЕВОГИ» В СИСТЕМАХ РАСПОЗНАВАНИЯ МВД 130

Д. А. Камаева, А. В. Серезевский
АНАЛИЗ СПОСОБОВ ОБХОДА ИЗВЕЩАТЕЛЕЙ В СОСТАВЕ СИСТЕМ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ, ПРИМЕНЯЕМЫХ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ 135

Д. Н. Саратов, В. А. Редковников
ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПРЕПОДАВАТЕЛЯ 139

А. Ю. Кузнецов, Ю. Е. Богомолова
PSYSCANNER – СОВРЕМЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ 142

Раздел 3. ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ 147

Н. В. Лукашов
О МЕЖВЕДОМСТВЕННОМ СИТУАЦИОННОМ ЦЕНТРЕ ПРОФИЛАКТИКИ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 147

Д. Б. Родионова, А. С. Овчинский
ПРОФИЛАКТИКА ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В ЦИФРОВОМ МИРЕ 151
В. В. Прудиус, Е. М. Шпагина
ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ СБОРА ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ 157
А. Д. Распутина, Е. В. Клянчина
ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ: АСПЕКТЫ ИСПОЛЬЗОВАНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ 162
О. С. Биккулова
АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: СИСТЕМА «ЛКС АНАЛИТИКА» 166
Д. Д. Савенкова
ОТДЕЛЬНЫЕ НАПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ФИНАНСОВО-КРЕДИТНЫХ УЧРЕЖДЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ 169
С. В. Гурдин
СОВЕРШЕНСТВОВАНИЕ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ТЕМЫ «ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» 179
М. П. Суханова
НЕОБХОДИМОСТЬ ВВЕДЕНИЯ ФАКУЛЬТАТИВА ПО КИБЕРБЕЗОПАСНОСТИ В НАЧАЛЬНОЙ И СРЕДНЕЙ ШКОЛЕ КАК ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ ... 184
Ж. В. Кустарева
МОДЕРНИЗАЦИЯ СИСТЕМЫ ОБРАЗОВАНИЯ В СВЯЗИ С РЕАЛИЗАЦИЕЙ ГОСУДАРСТВЕННОЙ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА» 188

Раздел 4. ПЕРСПЕКТИВНЫЕ МЕТОДЫ ИССЛЕДОВАНИЙ В ПРОТИВОДЕЙСТВИИ КИБЕРУГРОЗАМ 192

В. С. Власова
ОСОБЕННОСТИ НАЗНАЧЕНИЯ СУДЕБНЫХ ЭКСПЕРТИЗ ПО УГОЛОВНЫМ ДЕЛАМ О МОБИЛЬНЫХ МОШЕННИЧЕСТВАХ 192
В. И. Бокшицкий, И. С. Мельцева
МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ПРОИЗВОДНЫХ ПРИЗНАКОВ ОБЩЕСТВЕННОЙ ОПАСНОСТИ НЕЗАКОННОГО ОБРАЩЕНИЯ С КОНТРОЛИРУЕМЫМИ ТОВАРАМИ И ТЕХНОЛОГИЯМИ 196
В. Г. Любан
ОСОБЕННОСТИ РАБОТЫ БАНКОВСКИХ СЕРВИСОВ И ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ, ИСПОЛЬЗУЕМЫЕ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 206
Е. Л. Евраев, Д. Н. Захаров
МЕТОДИКА ИССЛЕДОВАНИЯ ОБРАЗОВ НЖМД С ЦЕЛЬЮ ПОИСКА СЛЕДОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ 213

Ю. А. Павенский, В. Ю. Иванов
МЕТОДЫ ИССЛЕДОВАНИЯ ДАМПОВ ОПЕРАТИВНОЙ ПАМЯТИ В ЦЕЛЯХ ОБНАРУЖЕНИЯ СЛЕДОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 219

В. В. Эльканов, Д. Н. Захаров, В. Н. Куликов
СРАВНЕНИЕ И АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ 226

А. В. Никифоров, Д. А. Кравченко
ФИКСИРОВАНИЕ ВЕРБАЛЬНЫХ ПРОЯВЛЕНИЙ КЛЮЧЕЙ ДОСТУПА К СКРЫТОЙ ИНФОРМАЦИИ КАК СПОСОБ РАЗОБЛАЧЕНИЯ ЗАМЫСЛА КИБЕРПРЕСТУПНИКОВ 230

А. В. Козырев, В. Ю. Иванов, А. О. Путилов
КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ RAID-МАССИВОВ ДАННЫХ 237

А. М. Тимофеева, В. Ю. Иванов
АНАЛИЗ МЕТОДОВ И СРЕДСТВ ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПОД ОС ANDROID 242

Л. М. Трибунский
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ДАННЫХ В МНОГОФАКТОРНОМ АНАЛИЗЕ СЛОЖНЫХ СИСТЕМ 246

М. Б. Кавешников
О ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОРГАНОВ ВНУТРЕННИХ ДЕЛ 252

Раздел 5. РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ 257

А. Г. Власюк, В. В. Гончар
ИСПОЛЬЗОВАНИЕ СЛЕДОВАТЕЛЕМ СОВРЕМЕННЫХ ЗНАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ 257

Е. Ю. Самолаева
ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ 263

В. А. Саморока, М. Ю. Бекетов, С. В. Гурдин
СПЕЦИФИКА ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ПОЗНАВАТЕЛЬНОЙ ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ 267

А. Ю. Петрунина, С. В. Ермаков
РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 272

М. А. Потапенко, С. В. Ермаков
РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ 278

А. А. Орлова
ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ ИЗ БАНКОВСКИХ АВТОМАТИЧЕСКИХ ТЕРМИНАЛОВ САМООБСЛУЖИВАНИЯ 282

В. И. Ткачева, Т. В. Радченко
ОСОБЕННОСТИ ДОПРОСА СВИДЕТЕЛЕЙ ПО ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ IT-ТЕХНОЛОГИЙ 290

М. В. Разинькова, В. Ю. Иванов
ПРОБЛЕМЫ ИЗЪЯТИЯ МОБИЛЬНЫХ УСТРОЙСТВ ПРИ ПРОВЕДЕНИИ СЛЕДСТВЕННОГО ДЕЙСТВИЯ «ОБЫСК» 295

П. Е. Власов
ОСОБЕННОСТИ ПРОИЗВОДСТВА ДОПРОСОВ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ МОБИЛЬНЫХ МОШЕННИЧЕСТВ 298

И. А. Гуляева, В. В. Гончар
ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПО ПРОИЗВОДСТВУ ОБЫСКА, СВЯЗАННОМУ С ИЗЪЯТИЕМ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ 303

Е. С. Юрченкова, В. В. Гончар
НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ 307

Н. Д. Тютлина, В. В. Гончар
АКТУАЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ НЕЗАКОННОГО ОБНАЛИЧИВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ ЧЕРЕЗ КРИПТОВАЛЮТУ 311

Н. К. Рудакова, В. В. Боровикова
ПРОБЛЕМЫ ПРИМЕНЕНИЯ ст. 110^2 УК РФ 317

А. Л. Прохоров, В. В. Гончар
ДЕЯТЕЛЬНОСТЬ СЛЕДОВАТЕЛЯ ПО ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИИ ИЗ БОРТОВОГО КОМПЬЮТЕРА АВТОМОБИЛЯ ПРИ РАССЛЕДОВАНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРЕСТУПЛЕНИЙ 321

Я. С. Городецкая, В. В. Гончар
ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СВЯЗИ С ПРИНЯТИЕМ ПОСТАНОВЛЕНИЯ ПЛЕНУМА ВЕРХОВНОГО СУДА РФ ОТ 30 НОЯБРЯ 2017 г. № 48 «О СУДЕБНОЙ ПРАКТИКЕ ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ, ПРИСВОЕНИИ И РАСТРАТЕ» 325

Н. В. Макеева, А. В. Макеева
ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РЕШЕНИИ ВОПРОСА О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО НЕЗАКОННОМУ СБЫТУ НАРКОТИЧЕСКИХ СРЕДСТВ БЕСКОНТАКТНЫМ СПОСОБОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ 329

С. В. Ермаков
УГОЛОВНОЕ СУДОПРОИЗВОДСТВО В СВЕТЕ РЕАЛИЗАЦИИ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА РОССИЙСКОЙ ФЕДЕРАЦИИ» 334

Раздел 6. ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ 339

А. В. Костюк, А. И. Примакин
К ВОПРОСУ ОБ ИНФОРМАЦИОННО- ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА 339

А. Н. Сударик, С. В. Здорова
ПСИХОЛОГИЧЕСКИЕ ПРЕДПОСЫЛКИ СОЦИАЛЬНОЙ НЕЗАЩИЩЕННОСТИ ГРАЖДАН В КОММУНИКАТИВНОЙ СФЕРЕ ПРИ ПРИМЕНЕНИИ ВЫСОКИХ ТЕХНОЛОГИЙ 343

Л. Б. Ткаченко
ИСПОЛЬЗОВАНИЕ ПРАВОНАРУШИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАСПРОСТРАНЯЕМЫХ ПОДРОСТКАМИ В СЕТИ «ИНТЕРНЕТ» 347

О. Ю. Карлина
НЕКОТОРЫЕ НЕГАТИВНЫЕ ФАКТОРЫ СЕТИ «ИНТЕРНЕТ», ФОРМИРУЮЩИЕ ЛИЧНОСТЬ ПОДРОСТКА-ПРАВОНАРУШИТЕЛЯ 352

К. Р. Аветисян
К ВОПРОСУ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННО- ПСИХОЛОГИЧЕСКИХ ВОЗДЕЙСТВИЙ 356

А. М. Голубкина
ЭМОЦИИ ЧЕЛОВЕКА: ВОЗМОЖНОСТИ ПРОВЕРКИ ИСКРЕННОСТИ 361

С. Ю. Капицын, А. Б. Менисов, И. А. Шастун
МЕТОДИКА ОЦЕНИВАНИЯ РЕЗУЛЬТАТИВНОСТИ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ 365

Н. В. Аникеева, А. С. Ропалло
ПСИХОЛОГИЧЕСКИЙ ПОРТРЕТ ПРЕСТУПНИКА В СЕТИ «ИНТЕРНЕТ» 370

Д. В. Деулин, А. В. Кравченко
ПЕРСПЕКТИВНАЯ ИНСТРУМЕНТАЛЬНО-ПСИХОЛОГИЧЕСКАЯ МЕТОДОЛОГИЯ ВЫЯВЛЕНИЯ СКРЫВАЕМОЙ ИНФОРМАЦИИ В РАМКАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ 378

И. А. Виноградова
ИСТОКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: ВЗГЛЯД С ПСИХОЛОГИЧЕСКОЙ ТОЧКИ ЗРЕНИЯ 383

И. В. Ульянова
ПРОСВЕТИТЕЛЬСКАЯ РАБОТА ИНСПЕКТОРА ПДН С НЕСОВЕРШЕННОЛЕТНИМИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ ПО ПРЕДУПРЕЖДЕНИЮ КИБЕРМАНИПУЛИРОВАНИЯ ЛИЧНОСТЬЮ В СОЦИАЛЬНЫХ СЕТЯХ 388

В. И. Алескеров
НЕКОТОРЫЕ СПОСОБЫ ВЫЯВЛЕНИЯ ЛИЦ, СОВЕРШАЮЩИХ КИБЕРПРЕСТУПЛЕНИЯ 395

Раздел 1. УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

А. С. Овчинский[1]

КРИМИНАЛЬНАЯ СРЕДА ЦИФРОВОГО МИРА КАК ИСТОЧНИК УГРОЗ КИБЕРБЕЗОПАСНОСТИ

Развитие представлений о криминальной среде. Подходя к кибербезопасности, мы, как правило, рассуждаем о защите информационных систем, раскрытии киберпреступлений, об астрономических суммах финансовых потерь и угрозах критически важным объектам, а также о количестве хакеров, которых по миру уже более сорока миллионов. Но мы не часто задаемся вопросом, откуда и как возникают армии преступников в нашем уже цифровом мире.

Заметим, что одним из фундаментальных достижений советской криминологии было создание научных представлений о криминальной среде. В условиях жесткой идеологии, которая требовала исчезновения преступности по мере построения коммунистического общества, оказалось, что криминальная среда функционирует и трансформируется, следуя своим внутренним закономерностям [1]. Она самосовершенствуется и саморазвивается, встраивается в общественные отношения. И, как показали уже лихие 90-е годы, криминальный мир даже подстраивает эти отношения под себя.

Под криминальной средой принято представлять некую часть общества (в определенной мере организованную, структурированную и даже сплоченную), которая включает преступников, их группы и формирования, кроме того личностей и даже целые слои населения, склонные к той или иной противоправной деятельности и асоциальному поведению.

Характерным признаком такой среды считается криминальная субкультура. Она охватывает обширный свод правил, традиций, специфические взаимоотношения и коммуникации. Здесь же определенные антиобщественные ценностные ориентации, вплоть до криминальных идеологий и мировоззрения.

Отмечалось также наличие как материальных, так и нематериальных ресурсов, создающих условия существования, самовоспроизводства и развития криминальной среды, возможности ее адаптации к изменяющимся условиям жизни общества и государственной политике.

---

[1] Профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя доктор технических наук, профессор. © Овчинский А. С., 2018.

Обратим внимание и на то, что криминальный мир оказался чрезвычайно восприимчивым к технологическим новациям. Около 15 лет назад отмечалось, что информационные технологии стали атрибутом самых разнообразных преступлений. Сегодня они открывают все более захватывающие криминальное воображение возможности обогащения и деструктивной деятельности.

Трудно представить криминальный бизнес, не использующий платформы Интернета. Преступная деятельность от хакерства, финансовых мошенничеств и распространения наркотиков до заказных убийств, терроризма и экстремизма все глубже погружается в информационные сферы. Криминальная среда со всеми ее архаичными атрибутами стремительно модернизируется и становится криминально-информационной.

Естественно, это требует адекватной реакции со стороны правоохранительных органов и как минимум научного осмысления. Так, не вполне осознаны угрозы общественной и национальной безопасности, связанные с криминогенными воздействиями на сознание молодежи. В недавние годы такие воздействия были связаны, например, с героизацией лидеров преступного мира, с внедрением силами искусства криминальных субкультуры и идеологии.

В наши дни заполнение электронного эфира экстремистскими идеями и призывами приводит к самовербовке в террористические и ультрарадикальные организации, созданию криминально ориентированных сетевых сообществ, таких как АУЕ (арестантский устав един), сетевых сообществ играющих экстремалов-правонарушителей, наконец, сообществ подростков, склоняемых к суициду. И это только то, что лежит на поверхности.

Криминология в цифровом мире. Современная криминология находится в глубочайшем кризисе. Она не может определить предмет своего исследования, обосновать, что же является преступным, а что не преступным. Ответ на эти вопросы дает уголовное право. То, что в уголовном праве фиксируется как наказуемое деяние, считается преступлением.

Но относительно недавно такие явления как, например, самогоноварение, употребление наркотиков, мужеложство… у нас в стране были уголовно наказуемыми. Сейчас они декриминализированы и, если не очень общественно поощряемы, то весьма популяризируемы.

В этой ситуации отметим еще одно фундаментальное достижение советской криминологии. На огромных массивах данных было уста-

новлено, что любому социально опасному, дерзкому, насильственному преступлению предшествует череда более мелких правонарушений: хулиганство, грубость, оскорбление женщин, жестокие драки, истязания животных, издевательства над слабыми. «Нарастание незначительных отступлений от позитивного (в социальном и нравственном плане) поведения приводит к антиобщественным и общественно опасным поступкам» [2].

Сегодня на передовую прогресса выходят системы искусственного интеллекта с технологиями распознавания и идентификации, с самообучающимися нейронными сетями, которые «пережевывают» и «переваривают» огромные массивы «больших данных».

Открывается возможность не только строить оцифрованные профили практически всех потенциальных правонарушителей и преступников, но и предсказывать вероятность, место и время того или иного преступления. Криминологическое прогнозирование и технологии обработки данных могут быть направлены на предотвращение преступлений и раннюю профилактику криминальных угроз [3].

Нельзя не коснуться зарубежного опыта. Так, немецкие эксперты говорят о четвертой промышленной революции, которая выводит и правоохранительную деятельность на качественно новый технологический уровень. В Англии создается правовая база цифровой экономики с приоритетом обеспечения кибербезопасности. Япония представила программу построения автоматизированного социально ориентированного и декриминализированного общества 5.0. Китай поражает темпами внедрения все более совершенных систем распознавания и биометрии [4].

В нескольких провинциях «Поднебесной» проходит масштабный эксперимент, в котором на основе оцифрованных профилей всем жителям начисляются положительные баллы за добропорядочное поведение и отрицательные – за хулиганство, ругань, курение и плевки в общественных местах. Эти баллы учитываются в уменьшении или увеличении суммы страховки, в величине процентов по кредитам, в предоставлении или лишении социальных льгот, в приеме на работу или в отказе в престижной работе.

Подходы к такой профилактике правонарушений можно встретить в самых ранних социальных утопиях. Мы же обратим внимание на то, что противостояние криминального мира и правоохранительных сил усилиивается именно в информационно-технологических и информационно-психологических сферах.

Система информационных координат. Для осмысления этого противостояния требуется своя система координат. Такую систему координат дает развитие представлений о триединстве реактивной, ресурсной и фоновой информации [5].

Реактивная информация возникает в процессе реакций на воздействия и побуждения, позволяя объектам природы выживать, а людям – понимать смысл происходящего и адекватно реагировать. Ресурсная информация фиксируется и накапливается как на природных, так и на искусственных носителях, передавая опыт выживания и социального развития. Фоновая информация, отражая окружающую реальность, обходит защитные функции сознания и включает механизмы адаптации.

Реактивность, ресурсность и фоновость составляют трехмерную систему универсальных координат, поскольку все явления нашей жизни так или иначе построены на информационных взаимодействиях.

Ресурсы криминальной среды – это огромные средства, поступающие от организованной преступности, от криминального контроля над экономикой, от наркобизнеса, незаконных видов деятельности.

Можно говорить о кадровых и технологических ресурсах, о подборе, вербовке и подготовке криминально ориентированных личностей, скажем, с незаурядными хакерскими способностями. Сюда же можно отнести и опыт успешных махинаций и использования передовых технологий, криминальных навыков и знаний, которые накапливаются и передаются новым поколениям преступников.

Фоновый вектор криминальной среды – это криминальная субкультура, обычаи, традиции, правила общения, ценностные ориентации, криминальная идеология.

Идеология не только как система взглядов, отражающих отношение к окружающей реальности, но и как система обоснования права (в данном случае на преступную деятельность).

К фону криминальной среды можно отнести и деформации общественных отношений, социально-экономическое неравенство, разрыв между реальными доходами населения и миллиардными состояниями.

Еще раз подчеркнем, именно фоновая проекция криминального мира, связанная с воздействиями на умы человечества, содержит наибольшие угрозы общественной стабильности и целым государствам, особенно с погружением в информационные сферы.

Наконец, реактивная проекция криминальной среды – это собственно преступления и преступная деятельность. Здесь уже можно рас-

крыть фрактальность или самоподобие информационных координат в анализе сложных систем. Эти координаты дают «мостики» перехода из одних сфер знания в другие.

В данном случае сформирован, условно говоря, информационный подход непосредственно к криминологии. Выделяются реактивные, ресурсные и фоновые преступления [6].

Реактивные преступления совершаются как некие противоправные преступные реакции на возникающие ситуации. Так, это многомиллионный массив бытовых преступлений (от пьяного водителя за рулем до мести «любимой» теще). В плане угроз кибербезопасности реактивные преступления обусловлены, например, компьютерной игроманией.

Американский хакер Верджил Гриффит в своих интервью объяснял, что «просвещенное мошенничество – это высшая форма игрового процесса». В свои 10 лет он разобрался в кодах компьютерной игры, клонировал нужных ему асов и «выигрывал» воздушные сражения. Сейчас (ему 34 года) он прямо утверждает, что «победа в хакерском мошенничестве – это вопрос принципа, вопрос чувства собственного достоинства. Более того, победа над наиболее сложной системой придает особое, ни с чем несравнимое чувство собственного превосходства» [7].

Опыт общения с молодыми хакерами, которые уже успехи побывать под следствием, также показывает, что все начиналось с гипертрофированного любопытства, с желания проверить свои возможности, с азарта соревнования, с игры, в которой стираются грани между реальностью и виртуальностью.

Но когда возникает страсть получить доступ к огромным финансовым средствам, мы имеем дело с ресурсными преступлениями.

В отличие от реактивной ресурсная преступность направлена непосредственно на получение криминальных доходов. Это огромный массив уже «настоящих» преступлений: от банальных краж, ограблений, разбоев до грандиозных финансовых махинаций, захвата собственности и ценностей в ходе социальных потрясений, экономических реформ, внешних интервенций.

Уровень доходов от преступлений в киберпространстве не только сопоставим, но и превосходит то, что дают другие виды криминального бизнеса. Все оценки преступных доходов приближенные, поскольку, заботясь о репутации и позиционируя себя надежными,

финансовые компании и банки стараются не афишировать потери от хакерских атак и финансовых мошенничеств.

На первый план выходит необходимость защиты информации. Но возникает вопрос: кто имеет больший доход? Те, кто покушается на информацию, или те, кто зарабатывает на ее защите?

Наконец, фоновая преступность – это некие, условно говоря, «идейные» преступления. Здесь мы сталкиваемся с терроризмом и экстремизмом во всем многообразии их проявлений.

Основоположники криминологического учения Чезаре Ламброзо [8] и Энрико Ферри [9] еще в XIX в. писали о необходимости выявлять и останавливать религиозных и политических фанатиков, которых страстная борьба довела до экзальтации и сделала убийцами.

Сегодня одновременно с броском в высоко технологическое будущее мир опускается в архаику языческих культов, человеческих жертвоприношений, показательных массовых казней с отрежиссированными голливудскими эффектами. И в этой архаике применение дронов, химических зарядов, боевых роботов и в целом новейших технологий позволяет небольшим группам (кланам, племенам, бандам) бросать вызов мировому сообществу [10].

Здесь же вырисовываются наибольшие угрозы кибербезопасности. Фоновая киберпреступность – это когда отдельные фанатики или их группы стремятся завладеть кодами управления атомных электростанций или пусковых установок баллистических ядерных ракет.

В целом проблема обеспечения кибербезопасности весьма многогранна. Ее разработка требует фундаментальных исследований, одним из объектов которых должна стать современная криминальная среда.

Библиографический список

1. Овчинский С. С. Преступное насилие. Преступность в городах / сост. и вступ. ст. А. С. Овчинского, В. С. Овчинского. – М. : Инфра–М, 2007.

2. Овчинский С. С. Оперативно-разыскная информация: монография / под редакцией А. С. Овчинского и В. С. Овчинского / 2-е изд., доп. – М. : Инфра–М, 2017.

3. Овчинский В. С. Технологии будущего против криминала. – М. : Книжный мир, 2017.

4. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. – М. : Норма: Инфра–М, 2018.

5. Овчинский А. С., Чеботарева С. О. Матрица преступности. – М. : Норма, 2006.

6. Овчинский А. С. Информационные воздействия и организованная преступность. – М. : Инфра–М, 2007.

7. Хефферман В. Хватит идеализировать хакеров, когда миром правят высокие технологии / общество / иносми – все, что достойно перевода. – http://inosmi. social/20180201/24/34/582/html.

8. Чезаре Ламброзо Новейшие успехи науки о преступнике. – М. : Инфра–М, 2004.

9. Энрико Ферри Уголовная социология. – М. : Инфра–М, 2005.

10. Пономарева Е. Г. Вывихнутый век. Кто его вправит? Хаос, конфронтация, интеграция. – М. : Книжный мир, 2016.

***Е. Н. Яковец*[1], *С. Ю. Окилов*[2], *Г. Г. Саркисян*[3]**

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Федеральным законом Российской Федерации от 21 декабря 2013 г. № 369-ФЗ «О внесении изменений в Федеральный закон «Об оперативно-розыскной деятельности» (далее ФЗ «Об ОРД») и ст. 13 Федерального закона «О федеральной службе безопасности» [1] был уточнен перечень социально значимых задач оперативно-разыскной деятельности, нашедших отражение в ст.ст. 2, 7, 8 и 15 ФЗ «Об ОРД». В настоящее время к их числу отнесено и добывание информации о событиях или действиях, создающих угрозу информационной безопасности Российской Федерации, которая является одним из ключевых элементов национальной безопасности страны.

Согласно положениям новой Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 [2], одной из первоочередных задач обеспечения информационной безопасности является «организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного (выделено нами – авторы), разведывательного, контрразведывательного, научно-техни-

---

[1] Профессор кафедры организации оперативно-разыскной деятельности Академии управления МВД России доктор юридических наук, профессор. © Яковец Е. Н., 2018.

[2] Адъюнкт кафедры организации оперативно-разыскной деятельности Академии управления МВД России. © Окилов С. Ю., 2018.

[3] Адъюнкт кафедры организации оперативно-разыскной деятельности Академии управления МВД России. © Саркисян Г. Г., 2018.

ческого, информационно-аналитического, кадрового и экономического обеспечения» [3].

Таким образом, обеспечение информационной безопасности является одной из главных задач оперативно разыскной деятельности, а в отдельных случаях – и ее основным результатом.

Как в этом контексте совместить содержание конкретных оперативно-розыскных мер с обеспечением информационной безопасности? Решение подсказывает приведенная выше выдержка из той же Доктрины, где отмечается, что наряду с оперативно-розыскными и прочими мерами поддержанию информационной безопасности призваны способствовать также меры информационно-аналитического характера. Этот посыл расставляет все точки над «i», отвечая на поставленный вопрос.

В свое время одним из авторов данной статьи высказывалась мысль о том, что качество информационно-аналитического обеспечения определяет характер информационной среды, в условиях которой оперативные сотрудники осуществляют свою деятельность. Состояние этой среды и является одним из трех основных факторов, оказывающих влияние на информационную безопасность в сфере ОРД. (Напомним, что второй элемент этого понятия связан с безопасностью информационных ресурсов, используемых в ОРД, а также информационно-коммуникационных систем, принадлежащих субъектам оперативно-разыскной деятельности, третий – с собственной информационной безопасностью последних. Эти направления деятельности обеспечиваются, в том числе и с помощью оперативно-разыскных мер) [4].

Рассмотрению содержания информационно-аналитического обеспечения ОРД посвящен целый ряд научных и учебно-методических работ одного из авторов данной статьи, в которых нашли отражение теоретические и прикладные основы информационно-аналитической деятельности в сфере ОРД ОВД [5]. В указанных работах содержится вывод о том, что оперативно-разыскной анализ, с одной стороны, является методологической основой ОРД, с другой – ее эффективным инструментарием, имеющим специфическую правовую регламентацию, организационное оформление и методику применения. Формы и методы аналитической работы, рассматриваемые в широком аспекте, пронизывают абсолютно все оперативно-разыскные меры, а сама информационно-аналитическая деятельность, умноженная на возможности, которые предоставляет координация усилий в данной области всех заинтересованных субъектов ОРД, в сочетании с другими эле-

ментами обеспечения информационной безопасности является одной из главных функций ее организации. Таким образом, оперативно-разыскная деятельность, как и любая другая профессиональная сыскная деятельность, неразрывно связывается с информационной безопасностью именно через осуществление информационно-аналитической работы.

Положения новой Доктрины информационной безопасности Российской Федерации практически целиком ориентированы на локализацию угроз, исходящих из киберпространства. Оставим за скобками вывод о том, что нынешнее видение информационной безопасности страны заметно сузилось по сравнению с тем, которое фигурировало в прежней Доктрине [6]. Видимо, разработчики нового документа, использовавшие данный подход, решили подобным образом подчеркнуть особую значимость противодействия информационным угрозам, исходящим из Интернет-пространства. И они абсолютно правы, поскольку данная область отношений является на сегодняшний день весьма чувствительной и проблемной с позиций обеспечения безопасности гражданского общества и государства.

С учетом подобной специфики поведем речь об оперативно-разыскных мерах, связанных с противодействием так называемым киберпреступлениям или компьютерным преступлениям (эти два термина, по мнению авторов, можно использовать как равнозначные), которые могут быть существенным образом активизированы за счет использования новейших информационно-аналитических технологий.

Однако вначале необходимо прояснить правовую природу киберпреступлений с информационной и уголовно-правовой точек зрения?

Как подчеркивают некоторые специалисты, единого понимания рассматриваемого вида преступлений современной наукой и практикой пока не выработано. В отечественных и зарубежным изданиях преступления, совершаемые в компьютерных и телекоммуникационных системах, интерпретируются по-разному: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», «киберпреступления», «преступления в сфере безопасности обращения компьютерной информации», «преступления в сфере компьютерной информации» и др. Такое терминологическое разнообразие понятий связано с отсутствием единого понимания специфики рассматриваемых преступлений, небольшим числом научных изысканий во всех сферах науки, направленных на изучение киберпреступлений [7].

Профессор А. Л. Осипенко характеризует совокупность рассматриваемых деяний как преступления в глобальных компьютерных сетях (сетевых компьютерных преступлений), которые ввиду многопланового механизма совершения требуют поиска новых криминалистических и оперативно-разыскных подходов к их выявлению, раскрытию и расследованию [8], а известный американский специалист по проблемам киберпространства Д. Л. Шиндер[9] за весьма пространные и «размытые» дефиниции, связанные с содержанием компьютерных преступных деяний, подвергает резкой критике даже Европейскую конвенцию о киберпреступности [10].

Еще один автор Э. Мелик отмечает в этой связи, что машинная информация одновременно рассматривается и в качестве объекта, и в качестве орудия преступления. Наряду с ней в разряд орудий совершения подобных преступлений попадают сам компьютер, а также информационно-телекоммуникационная сеть (вычислительная среда, в которой эта информация циркулирует). С учетом сказанного, по ее мнению, можно выделить следующие характерные особенности компьютерного преступления: неоднородность предмета посягательства; особенности машинной информации, рассматриваемой как в качестве предмета, так и в качестве средства (орудия) совершения преступления; многообразие предметов и средств преступного посягательства; особенности компьютера и компьютерной сети в целом, рассматриваемых и в качестве предметов, и в качестве средств совершения преступления. Поэтому в качестве основного классифицирующего признака принадлежности преступления к разряду компьютерных следует выделить словосочетание «использование средств компьютерной техники», независимо от того, на какой стадии преступления она использовалась: при его подготовке, в ходе совершения или для сокрытия [11].

Авторы данной статьи, соглашаясь с высказанными точками зрения, полагают, тем не менее, что киберпреступления являются одной из разновидностей так называемых информационных преступлений, в связи с чем под компьютерными преступлениями (киберпреступлениями) следует понимать предусмотренные уголовным законом общественно опасные деяния, посягающие на информационную безопасность личности, общества и государства, совершенные с использованием средств электронно-вычислительной (компьютерной) техники.

По итогам прошлого года в России было зарегистрировано 90587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. Из них раскрыто только 20424 [12], т. е. 22,5 %.

Основную часть этих преступлений – до 80 % – составляют хищения, из которых 61,1 % – кражи; 22,3 % – мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ); 9,1 % – присвоение и растрата; 7,5 % – грабежи и разбои [13].

Наряду с этим весьма актуальным на сегодняшний день представляет противодействие оперативных аппаратов полиции следующим видам компьютерных преступлений, причиняющих наиболее существенный вред охраняемым общественным отношениям:

– распространению через Интернет материалов экстремистского характера, подпадающее под признаки ст. 282^1 УК РФ (организация экстремистского сообщества) и ст. 282^2 УК РФ (организация деятельности экстремистской организации);

– сбыту наркотических средств, психотропных веществ или их аналогов, совершенному с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», квалифицируемому по признакам ст. 228^1, ч. 2, п. «б» (незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества);

– распространению или обороту с помощью сети «Интернет» порнографических материалов, подпадающих под признаки п. «б» ч. 3 ст. 242 (незаконные изготовление и оборот порнографических материалов или предметов), п. «г» ч. 2 ст. 242^1 УК РФ (изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних), а также п. «г» ч. 2 ст. 242^2 УК РФ (использование несовершеннолетнего в целях изготовления порнографических материалов или предметов).

Высокую общественную опасность представляет организация с помощью Интернета заказных убийств [14], а также склонение к суициду, в которое вовлекаются главным образом представители юного поколения.

На распространение в Интернете сайтов, пропагандирующих самоубийства, особое внимание обратил даже Президент нашей страны В. В. Путин, выступая на расширенном заседании коллегии Министерства внутренних дел Российской Федерации 9 марта 2017 г. Подчеркнув, что действия лиц, совершающих подобные преступления, прежде всего нацелены на подростковую и молодежную аудитории, на детей с неокрепшей психикой или находящихся в трудной жизненной

ситуации, Президент призвал к самому решительному противодействию подобным криминальным проявлениям [15].

Выявление преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации, в том числе сети «Интернет» и сетях мобильной связи, возложены главным образом на сотрудников подразделения «К» Бюро специальных технических мероприятий МВД России и его подразделений на местах. Выявление и раскрытие мошенничеств в банковской сфере возложено на подразделения уголовного розыска. По мнению многих специалистов, существующая в настоящее время штатная численность и материально-техническое обеспечение специализированных подразделений МВД России, противодействующих киберпреступлениям, не позволяют эффективно бороться с ними [16].

Еще более категоричен в своих выводах известный российский криминолог В. С. Овчинский, анализирующий зарубежный опыт борьбы с подобными видами преступлений. По его данным, свыше 80 % выявленных в мире киберпреступлений связаны с организованной преступностью. Причем «добыча» одного среднего киберпреступника в семь раз превышает «добычу» обычного преступника. В Нью-Йорке раскрываемость обычных общеуголовных преступлений составляла в разные годы от 40 до 60 %, а киберпреступлений – всего 4 %. Иными словами, киберпреступность – это высокодоходная и мало рискованная криминальная деятельность.

Между современной и старой, традиционной преступностью, по мнению указанного ученого, имеется не только антагонизм, но и существенная разница в методах и организации преступных синдикатов. Современные криминальные кланы уже отказываются от традиционных иерархических пирамид времен дона Карлеоне и Тони Сопрано и формируют более мобильные сетевые структуры. Они активно используют аутисорсинг, коллективное предпринимательство, платформенные решения и т. п. Одним словом, если преступники до середины XX в. «плелись в хвосте» технических, организационных и финансовых технологий, то сегодня они, несомненно, находятся в авангарде.

Приоритетным, с точки зрения современного криминалитета, является использование так называемого «искусственного интеллекта», гарантирующего высокую прибыльность преступного бизнеса в сочетании с низким уровнем риска. В связи с этих ФБР ведет основательную подготовку к появлению, например, подпольного синдиката, специализирующегося на заказных высокотехнологичных убийствах, замас-

кированных под технические инциденты различного рода, а также использованию искусственного интеллекта для разведывательной деятельности организованной преступностью против полиции и ФБР.

По данным американских силовых структур, криминальные «мозговые центры» начали создание собственных баз данных, формируемых с использованием искусственного интеллекта, аналогичных тем, которыми располагают правоохранительные органы. По данным ФБР, преступники наряду с прочими аспектами применения новейших информационных технологий в криминальных целях намерены организовать анализ потокового видеоизображения в местах расположения правоохранительных органов с целью распознания и отождествления агентов под прикрытием и лиц, оказывающих содействие полиции. Кроме этого прогнозируются попытки выявления представителями криминалитета сотрудников информационно-аналитических центров полиции и ФБР, владеющих важнейшими сведениями о борьбе с преступностью.

Силовые структуры США и других западных стран, осознавая масштабы киберугроз, активно прорабатывают меры противодействия им [17].

На этом фоне, – подчеркивает В. С. Овчинский, – в нашей стране концепция борьбы с киберпреступностью отсутствует, и уже сейчас становится очевидным, что правоохранительная система в своих ответных действиях на технологизацию преступного мира запаздывает. Чтобы это запаздывание не оказалось фатальным, необходима коренная перестройка всей системы подготовки кадров правоохранительных структур и их привлечения на службу в интересах борьбы с киберпреступностью. По существу в ближайшее десятилетие вся обычная полиция должна стать одновременно и киберполицией, использующей новейшие достижения в работе с «большими данными», по сбору иной представляющей интерес информации и ее анализу [18].

Другими словами, заинтересованным отечественным службам есть о чем задуматься, а новая Доктрина информационной безопасности Российской Федерации призвана сыграть в решении обозначенных проблем роль катализатора.

Кстати, активизации борьбы с киберпреступностью призван способствовать и еще один знаковый законодательный акт, именуемый в обиходе «Законом Яровой» [19], который дополнил перечень ОРМ, фигурирующий в ч. 1 ст. 6 ФЗ «Об ОРД», новым оперативно-розыскным мероприятием – «получение компьютерной информации».

Что же касается применения оперативными подразделениями полиции автоматизированных логико-аналитических систем, использующих технологии «искусственного интеллекта», то разговор об этом среди российских ученых ведется уже давно [20], однако проблема эта в полной мере пока не решена.

Киберпреступность стремительно обретает характер транснационального, глобального зла. Генеральная Ассамблея ООН еще в своих резолюциях 53/70 от 4 декабря 1998 г. и 54/49 от 1 декабря 1999 г. поставила вопрос о целесообразности разработки международных принципов, направленных на усиление безопасности глобальных информационных и телекоммуникационных систем, борьбы с информационным терроризмом и преступностью.

23 ноября 2001 г. представители стран-членов Совета Европы, США, Канады, Японии и ЮАР подписали Конвенцию о преступности в сфере компьютерной информации. В Совете ЕС создано специальное «Агентство информационной безопасности».

Разрабатываются превентивные меры в этой области и на постсоветском пространстве. Так, в современном Таджикистане, как и в некоторых других бывших союзных республиках СССР, организованная преступность распространила свое влияние на многие сферы жизнедеятельности общества, в том числе и на киберпространство. Наиболее уязвимой при этом оказалась банковская сфера, где весьма распространенным явлением является незаконное завладение денежными средствами физических и юридических лиц.

Чтобы эффективно противодействовать киберпреступлениям в банковской сфере Таджикистана, необходимо прежде всего определиться с оперативно-разыскной характеристикой данного вида преступлений.

Существуют различные подходы к понятию «оперативно-разыскная характеристика преступлений», однако, наиболее емким, на наш взгляд, является понятие, введенное в научный оборот профессором Д. В. Гребельским, который понимал под ней совокупность ряда устойчивых и взаимообусловленных информационных признаков криминалистического, психологического, экономического и иного характера, содержание которых в совокупности способствует обоснованному выдвижению и проверке оперативно-разыскных версий при раскрытии родовых групп или отдельных видов преступлений [21].

Аналогичные точки зрения высказывали впоследствии профессора А. М. Абрамов, И. А. Климов, В. В. Гордиенко и П. И. Иванов [22] и др. Данная формулировка позволяет правильно определить основные

направления деятельности правоохранительных органов, объекты и способы эффективного применения сил, средств и методов оперативно-разыскной деятельности, а также дает возможность не только успешно выявлять, предупреждать и раскрывать преступления, но и обеспечивать оперативное сопровождение уголовного судопроизводства. Из определения, сформулированного Д.В. Гребельским, следует, что надлежащее знание оперативно-разыскной характеристики способствует не только наиболее эффективному раскрытию отдельных преступлений, но и целых их родовых групп. В нашем случае такую родовую группу образуют противоправные деяния, связанные не только с киберпреступлениями в банковской сфере, но и компьютерными преступлениями, совершаемыми в других сферах общественных отношений.

Высказанные Д. В. Гребельским мысли актуальны применительно к исследованию информационных особенностей оперативно-разыскной характеристики преступления, которые включают в себя признаки «криминалистического, психологического, экономического и иного характера» [21].

В рамках предлагаемой оперативно-разыскной характеристики киберпреступлений необходимо выделить вопросы уголовно-правовых, криминологических и криминалистических особенностей рассматриваемых преступлений, способствующих более глубокому пониманию влияния преступного посягательства рассматриваемого вида, оказываемого на информационную безопасность. Это позволяет в конечном счете отграничить данное преступное деяние от иных информационных преступлений.

С учетом сказанного можно предложить следующую формулировку оперативно-разыскной характеристики киберпреступлений в банковской сфере (применительно к специфике Республики Таджикистан). Оперативно-разыскная характеристика киберпреступлений в банковской сфере представляет собой ряд устойчивых и взаимосвязанных информационных признаков уголовно-правового, криминологического, криминалистического характера, а также иных специальных признаков[1], знание которых способствует наиболее эффективной организации и тактике оперативно-разыскной деятельности органов внутренних дел Республики Таджикистан по противодействию указанным преступным деяниям.

---

[1] К иным специальным признакам можно отнести собственно оперативно-разыскные, психологические, экономические признаки и др.

Библиографический список

1. Российская газета. – 2013. – 25 декабря.
2. Российская газета. – 2016. – 6 декабря.
3. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета. – 2016. – 6 декабря. П. 2, пп. «в», «г»; п. 35, пп. «г».
4. Яковец Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации: учебное пособие. 2-е изд., доп. и перераб. – М. : Юрлитинформ, 2014. С. 305.
5. Яковец Е. Н. Проблемы аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел : монография. – М. : Издательский дом И. И. Шумиловой, 2005; Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учебное пособие. – М. : Щит-М, МосУ МВД России, 2009; Яковец Е. Н. Аналитическое обеспечение оперативно-розыскной деятельности (т. 4) // И. М. Даукаев, Н. И. Журавленко, А. Н. Халиков, Е. Н. Яковец. Правовое, техническое и аналитическое обеспечение оперативно-розыскной деятельности по борьбе с коррупционными преступлениями: монография. В 4 т. – Уфа : РИЦ БашГУ, 2013.
6. Доктрина информационной безопасности Российской Федерации (9 сентября 2000 г. Пр-1895). Утратила силу 6 декабря 2016 г. // Российская газета. – 2000.– 29 сентября. Разд. I, п. 1
7. Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис.… канд. юрид. наук. – М. : МГЮА, 2016. С. 14.
8. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. С. 109-110.
9. Scene of the Cybercrime: Computer Forensics Handbook by Debra Littlejohn Shinder, Ed Tittel (Editor). 2002 / пер. с англ. Т. Тропиной. Владивосток: ВЦИОП при Юридическом институте ДВГУ, 2003. С. 4.
10. Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001г. / URL: http://www. lawmix. ru/abro. php?id=3454 (дата обращения: 24.08.2016).
11. Мелик Э. Компьютерные преступления: URL: http://www. melik. narod. ru/ (дата обращения: 09.01.2017).
12. Состояние преступности в России за январь – декабрь 2017 г. – М. : ГИАЦ МВД России, 2018. С. 3.
13. Мазуров И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий : автореф. дис. … канд. юрид. наук. Ростов-на-Дону : Ростовский ЮИ МВД России, 2017. С. 3.

14. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений // URL: http://kkrimlguvd. org. ua/ conferences/article/3 (дата обращения: 07.07.2016).

15. Путин В. В. Выступление на расширенном заседании коллегии МВД России 9 марта 2017 г. // URL: http://путин.ru-an.info/новости/выступление-владимира-путина-на-расширенном-заседании-коллегии-мвд-россии/ (дата обращения: 10.03.2017).

16. Иванова А. А. Методика расследования незаконного изготовления, распространения и оборота порнографических материалов или предметов: дисс.... канд. юрид. наук. – Псков: ПЮИ ФСИН России, 2011. – С. 165.

17. Овчинский В. С. Трамп, ФБР, искусственный интеллект: основные направления стратегии по обеспечению кибербезопасности / Завтра // 2017. 6 февраля: URL // http://zavtra.ru/blogs/tramp_ fbr_iskusstvennij_intellekt (дата обращения: 14.02.2017).

18. Овчинский В. С. Преступность. Футурологический взгляд // http://zavtra. ru/ blogs/prestupnost (дата обращения: 14.02.2017).

19. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности. Федеральный закон от 6 июля 2016 г. № 374-ФЗ. Ст. 3 // Российская газета. – 2016. – 8 июля.

20. Губин А. В., Хлуднев П. Н., Яковец Е. Н. Современные подходы к информационно-аналитическому обеспечению оперативно-розыскной деятельности органов внутренних дел // Информатизация и информационная безопасность правоохранительных органов: Сборник трудов XII международной конференции 20-21 мая 2003 г. – М. : Академия управления МВД России, 2003. – С. 188-192: Кузнецов И. П., Шарнин М. Н., Золотарев О. В. Экспертные решения на основе взаимосвязанных объектов // Системы и средства информатики. Вып. 7. – М., 1995. – С. 119-125.

21. Гребельский Д. В. О состоянии криминалистических и оперативно-разыскных характеристик преступлений // Криминалистическая характеристика преступлений. – М ., 1984. – С. 75.

22. Абрамов А. М., Климов И. А. К вопросу о содержании оперативно-разыскной характеристики вида преступлений // Актуальные вопросы борьбы с преступностью и проблемы преподавания : сб. науч. трудов. – М., 1996. – С. 78-87; Гордиенко В. В. Правовые, организационные и тактические основы раскрытия разбоев и грабежей личного имущества, совершенных преступными группами : автореф. дис.… канд. юрид. наук. – М., 1983. – С. 14; Иванов П. И. Оперативно-разыскная деятельность органов внутренних дел по борьбе с экономическими преступлениями в сфере агропромышленного комплекса: вопросы теории и практики : автореф. дис.… д-ра юрид. наук. – М., 2000. – С. 23.

Ю. И. Синещук[1]

СИСТЕМОЛОГИЧЕСКИЙ АНАЛИЗ БАЗОВЫХ ПОНЯТИЙ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Повышение роли информация и информационных технологий в различных областях деятельности, включая и правоохранительную, является важнейшей тенденцией, определяющей облик человечества в современном мире.

Доктрина информационной безопасности Российской Федерации указывает, что «*Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства*»[2].

Вместе с тем, надо учитывать, что научно-технический прогресс, появление и внедрение электронных, сетевых технологий помимо позитивных аспектов, влечет еще и негативные последствия, в частности, появления и распространения информационных, а в более широком плане – киберугроз.

В Доктрине отмечается, что «*возможности трансграничного оборота информации все чаще используются для достижения… террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности… Возрастают масштабы компьютерной преступности, при этом методы, способы и средства совершения таких преступлений становятся все изощреннее*». Специалисты отмечают, что количество преступлений в киберпространстве растет самыми быстрыми темпами. Именно поэтому в деятельности МВД России значительное внимание уделяется проблеме борьбы с киберпреступностью, действиям в условиях информационного противоборства[3]. При этом киберпространство с его технологичными возможностями должно восприниматься не только как современное средство коммуникации и обработки информации в преступных целях, но и как эффективное средство предупреждения киберпреступлений.

В условиях динамичности защищаемой среды и угроз целесообразна реализация концепции адаптивной кибербезопасности.

---

[1] Профессор кафедры специальных информационных технологий ФГКОУ ВО «Санкт-Петербургский университет МВД России». © Синещук Ю. И., 2018.

[2] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

[3] Синещук Ю. И., Суслин А. В., Примакин А. И., Бобонец С. А. Особенности и задачи подготовки специалистов МВД в области информационных систем и технологий // Вестник Санкт-Петербургского университета МВД. – 2016. – № 2. – С. 130–136.

Очень часто термин «кибербезопасность» не выделяется из объема понятия «информационная безопасность», ассоциируется с ним. В то же время в большинстве зарубежных стран он выделен в самостоятельную дефиницию, а учитывая трансграничность киберпространства целесообразно в первую очередь определить единые базовые понятия и термины. Вопросы кибербезопасности прочно вошли в международные сообщество, чем и определилось появление международного стандарта ИСО/МЭК 27032: 2012, который, как правило, и берется за основу при исследовании вопросов кибербезопасности[1].

Понятие кибербезопасности естественным образом пересекается с понятием киберпространство. Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм человеческой активности (личности, организации, государства), осуществляемой посредством их использования.

Киберпространство можно рассматривать как триаду, которая включает в себя три основные составляющие: информация, техническая инфраструктура, ИТ, программное обеспечение и информационное взаимодействие[2].

Киберпространство, как сложная система, предполагает реализацию свойств организованности и управляемости, которые способны придать киберпространству способность реализации соответствующих функций и устойчивость к возникающим угрозам. Особенностью киберпространства является необыкновенно высокая и все нарастающая интенсивность атак, обусловленная масштабом киберпространства, множественностью всевозможных и разнохарактерных связей между ними.

Стоит отметить, что еще в 2002 г. ООН приняло резолюцию по созданию глобальной культуры кибербезопасности, определив основные элементы: осведомленность; ответственность; реагирование; этика; демократия; оценка риска; проектирование и внедрение средств обеспечения безопасности; управление обеспечением безопасности; переоценка.

По данным компании «Лаборатория Касперского», 9 из 10 компаний сталкиваются с внешними киберугрозами. Более того, почти поло-

---

[1] ИСО/МЭК 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for Cybersecurity).

[2] Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятий // Вопросы кибербезопасности. – 2014. – № 1 (2).

вина участников исследования утверждает, что количество кибератак увеличилось. Если проанализировать известные инциденты с информационной безопасностью (NASA, Sony, RSA, Lockheed Martin, Gazprom), можно сделать вывод, что традиционные подходы не полностью соответствуют современным вызовам киберпреступности и необходимо переходить на новые принципы и средства безопасности нового поколения. При этом важно правильно сформулировать понятие кибербезопасности, чтобы главные цели работы служб и средств защиты киберпространства от возникающих угроз были точно определены. Кибербезопасность можно определить как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями, обеспечивая максимально благоприятную среду для работы пользователей и всех систем[1]. Киберпреступники пользуются преимуществами быстрого расширения сферы их атак. Сегодня уже можно констатировать, что наступило время не просто киберпреступлений, а кибертерроризма и кибервойн.

Киберпреступность – преступная деятельность, в которой техническая инфраструктура киберпространства используется в целях преступления или является целью, преступления, или где киберпространство является источником, инструментом, целью или местом преступления.

Кибертерроризм – комплекс незаконных действий, создающих угрозу государственной безопасности, личности и обществу. Основной целью кибертерроризма является получение преимущества в решении социальных, экономических и политических задачах. Если в совершении подпадающих под это определение действий принимают участие представители правительственных или иных государственных структур, это считается проявлениями кибервойны. Поскольку кибертерроризм носит трансграничный характер, его проявления могут привести к ухудшению отношений между государствами, нарушить экономические и дипломатические связи, затруднить работу межгосударственных организаций. Это может полностью разрушить выстроенную систему международных отношений, вызвать панику в обществе и затруднить возможности организованно противостоять преступности. В связи с развитием технологий угроза кибертерроризма постепенно сравнивается по значимости с остальными его проявлениями.

[1] Кибербезопасность. http://mindstep. ru/wiki/index. php.

Д. Н. Шурухнова[1]

ОПЫТ ЕВРОПОЛА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Европейский союз предоставляет своим гражданам пространство свободы, безопасности и правосудия без внутренних границ, в рамках которого обеспечивается свободное передвижение лиц во взаимосвязи с соответствующими мерами по вопросам контроля внешних границ, предоставления убежища, иммиграции, а также предотвращения преступности и борьбы с этим явлением[2].

Особенностью пространства свободы, безопасности и правосудия Европейского союза является то, что помимо функционирования национальных правоохранительных органов координация осуществляется специально созданными европейскими учреждениями, такими как Европейское полицейское ведомство – Европол, Евроюст, Европейское ведомство по борьбе с мошенничеством – ОЛАФ, основной целью деятельности которых является установление сотрудничества в сфере борьбы с преступностью[3]. Европейское полицейское ведомство рассматривается прежде всего в качестве одного из ключевых элементов в пространстве свободы, безопасности и правосудия.

Правовой основой деятельности Европола с 1 мая 2017 г. является Регламент Европейского парламента и Совета ЕС 2016/794 от 11 мая 2016 г. об агентстве ЕС по сотрудничеству в правоохранительной сфере (Европол)[4], который заменил действовавшее ранее Решение 2009/371/ПВД Совета от 06.04.2009 о создании Европейского полицейского ведомства – Европол (Europol).

Принятие Регламента 2016/794 от 11 мая 2016 г. указывает на желание расширить и усилить полномочия правоохранительных органов в рамках Союза. Впервые правовой статус Европола закреплен Регламентом, который среди источников вторичного права занимает первое

---

[1] Профессор кафедры административного права МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Шурухнова Д. Н., 2018.

[2] Статья 3 Договора о Европейском союзе (Подписан в г. Маастрихте 07.02.1992) (с изм. и доп. от 13.12.2007).

[3] Сорокина Е. М. Правовые основы компетенции Европейского союза в области пространства свободы, безопасности и правосудия на современном этапе // Актуальные проблемы российского права. – 2015. – № 7 (56). – С. 204.

[4] Regulation (EU) 2016/794 of the European parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/ JHA and 2009/968/JHA // Official Journal of the European Union, 24.05.2016, L. 135, P. 53-114.

место, т. к. имеет общее действие, прямое применение и обязательный характер.

В регламенте отмечается, что многопрофильность и трансграничность преступных группировок представляют серьезную угрозу для безопасности ЕС и его граждан. В связи с этим правоохранительные органы должны более тесно сотрудничать, в чем Европол должен оказывать всемерную поддержку.

На Европол возлагаются задачи по осуществлению анализа и оценки угроз в правоохранительной сфере в целях определения стратегических и оперативных направлений ЕС по борьбе с преступностью (п. 7).

Назначением Европола, согласно статье 88 Договора о функционировании Европейского союза[1], являются поддержка и усиление деятельности полицейских органов и иных правоохранительных служб государств-членов, а также их взаимного сотрудничества в предотвращении и противодействии тяжкой преступности, затрагивающей два или большее число государств-членов, терроризма, а также тех форм преступности, которые посягают на общие интересы.

Согласно Стратегии Европола на 2016–2020 гг. основные цели деятельности остаются неизменными и будут ориентированы на всемерную поддержку развития эффективного сотрудничества между правоохранительными органами ЕС в борьбе с тяжкими преступлениями, организованной преступностью и терроризмом.

Технологические инновации в современных условиях могут использоваться как в социально полезных, так и в противоправных целях. Одним из негативных проявлений технологического прогресса является преступность в сфере высоких технологий. Раскрытие и расследование преступлений в сфере высоких технологий предполагают необходимость привлечения специалистов, обладающих экспертными познаниями. Сама преступность имеет трансграничный характер, получает все большее распространение, обладает высокой общественной опасностью[2].

Преступления в сфере высоких технологий представляют собой серьезную растущую угрозу порядку и безопасности в государствах-

---

[1] Договор о функционировании Европейского союза (Подписан в г. Риме 25.03.1957) (с изм. и доп. от 13.12.2007).

[2] Цалко Н. В., Мерецкий Н. Е. Преступления в сфере высоких технологий экономической направленности // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. Том 3. – Хабаровск, 2012. – С. 293–299.

членах ЕС, в которых развита интернет-инфраструктура, а платежные системы переведены в режим онлайн.

В целях совместной борьбы с преступлениями в сфере высоких технологий в Европоле с 1 января 2013 г. функционирует Европейский центр борьбы с киберпреступностью (European Cybercrime Centre – EC3).

В рамках Центра сформирована в сентябре 2014 г. Совместная спецгруппа по борьбе с киберпреступностью (Joint Cybercrime Action Traskrorce – J-CAT), осуществляющая разведывательную и аналитическую деятельность в сфере высоких технологий. В рамках J-CAT организуются и проводятся совместные операции и расследования, направленные на координацию действий в борьбе с угрозами киберпреступности.

Ежегодно EC3 проводит оценку угроз организованной преступности в Интернете (Internet Organised Crime Thereat assessment – IOCTA). Оценка содержит ключевые рекомендации правоохранительным органам в целях эффективной борьбы с киберпреступностью. Основное внимание в последние годы уделяется борьбе с киберзависимыми преступлениями, интернет-сексуальной эксплуатацией детей, мошенничеством в сфере платежных систем, онлайн-криминальными рынками, а также противодействию использования высоких технологий при совершении террористических актов.

Оценка включает в себя: основные выводы экспертов за отчетный год; прогноз тенденций и ситуаций в рассматриваемой сфере; рекомендации заинтересованным субъектам по противодействию угрозам в сфере высоких технологий.

Кроме того, отчет содержит краткий географический обзор ситуации по борьбе с киберпреступностью по всем пяти континентам.

В качестве примера успешной совместной борьбы с преступлениями в сфере высоких технологий следует указать операцию, проведенную 30 ноября 2016 г. с участием Европола по ликвидации сети Avalanche, которая использовалась для запуска и управления массовыми атаками вредоносного ПО. Следует отметить, что данная операция явилась результатом четырехлетнего расследования. По экспертным оценкам, данная платформа причинила убытки в размере 6 млн евро онлайн банковской системе в одной только Германии, а потери, связанные с атаками вредоносного ПО, проводимые по сети Avalanche по всему миру, оцениваются в сотни миллионов евро[1].

[1] Официальный сайт Европола: www. europol.europa.eu.

В июне 2017 г., была проведена успешная совместная операция с участием Европола по ликвидации двух крупных рынков Darknet: AlphaBay и Hansa, на которых осуществлялась торговля более 350 тыс. нелегальных товаров, включая наркотики, оружие и вредоносные ПО для киберпреступлений. Экспертами операция признается одной из самых сложных, которая когда-либо проводилась по борьбе с преступными действиями в Интернете.

Деятельность правоохранительных органов по выявлению киберпреступлений, их квалификации, сопряжены с большим количеством сложностей технического плана, во многом зависят от фактора времени и квалификации сотрудников правоохранительных органов. Таким образом, эффективная борьба с преступлениями в сфере высоких технологий возможна при наличии единых прозрачных международных инструментов, основанных на внедрении новых организационных форм сотрудничества в данной сфере[1]. Борьба с преступлениями в сфере высоких технологий предполагает особый подход в подготовке специалистов правоохранительных органов[2].

Преступления в сфере высоких технологий представляют собой трансграничную угрозу, предопределяющую необходимость тесного полицейского сотрудничества. Борьба с преступлениями, не имеющими границ, в большей степени предполагает необходимость тесной кооперации всей системы правоохранительных органов как в региональных, так и международных масштабах. Использование опыта Европола в борьбе с преступлениями в сфере высоких технологий требует глубокого изучения в целях определения возможности его использования в рамках межгосударственного полицейского сотрудничества на постсоветском пространстве.

---

[1] Зиборов О. В., Иванов М. А., Чекунов И. Г. Состояние кибербезопасности современного информационного общества // Вопросы кибербезопасности. – 2017. – Т. 2. – № 2 (20). – С. 15–18.

[2] Калиниченко И. А. Практико-ориентированный подход к подготовке специалистов в области кибербезопасности // Вопросы кибербезопасности. – 2017. – Т. 2. – № 2 (20). – С. 3–6.

В. Г. Бурлов[1]

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ ВОЙНЫ

Критически важным ресурсом, оказывающим определяющее влияние на национальную безопасность, становится информация, циркулирующая в обществе. В процессе деятельности социально-экономические образования различного уровня иерархии (от отдельного человека, организации, района до государства) при несовпадении целей деятельности возникают конфликты. В основе деятельности лежит решение человека (лица принимающего решение – ЛПР). Сама деятельность основывается на модели [1, 2]. Под информацией обычно понимают сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством. Сведения, используемые человеком в своей деятельности, имеют у него модельную интерпретацию процессов окружающего мира. Зависимость деятельности человека от информации (модельного представления) сформировала новое направление в противоборстве социально-экономических образований как информационное, которое в конце XX в. получило название «информационная война» (ИВ). Для решения комплекса задач ИВ необходимо разработать теорию [7]. Правильно построенная теория имеет три уровня, три составляющих. Методология. Методы. Технология. ЛПР воспринимает окружающий мир и осуществляет свою деятельность через процессы. Процесс – это объект в действии при фиксированном предназначении [2, 4]. Конструктивная методология должна формировать условие существование процесса, с которым работает ЛПР [2, 4]. В публикациях обычно рассматривают отдельные задачи ИВ. Конструктивные методологические основы в завершенном виде, в форме условия существования процесса, с которым работает ЛПР, в публикациях не представлены. Не располагая методологическими основами решения задач ИВ в форме условия существования процесса, мы не можем гарантировать достижение цели деятельности. Поэтому задачи ИВ решались и решаются на основе необходимых условий. То есть при допущении, что предполагаемое решение существует. Такая ситуация породила фундаментальную проблему: «Результаты деятельности при решении задач ИВ не оправдывают ожидания ЛПР». Рассмотренная совокупность

[1] Профессор кафедры специальных информационных технологий Санкт-Петербургского университета МВД России. © Бурлов В. Г., 2018.

факторов определяет актуальность настоящей работы, а целью является выбор и обоснование условия существования процесса ИВ в интересах гарантированного достижения цели деятельности ЛПР.

Постановка задачи. Человек решает задачи на основе трех категорий. Это Система. Модель. Предназначение [1, 2, 4]. Деятельность осуществляется в трех системах: социальной, экономической, технико-технологической. Поэтому ИВ строится на воздействии на процессы, протекающие в этих системах. Социальная и экономическая системы разрушаются через индивидуальное и массовое сознание, а технико-технологическая – через технические средства, в первую очередь компьютеры. Как это происходит и почему, мы это выясним в настоящей работе. Поэтому для успешного решения задач ИВ надо разрешить две проблемы методологического уровня.

Проблема 1. Для разработки системы известно два подхода. Разработка системы на основе анализа (перебор вариантов). Разработка системы на основе синтеза (требует знания закона построения и функционирования системы). Обычно используется первый подход. Но он не позволяет гарантировать достижение цели. Автором настоящей работы для решения проблемы 1 предлагается использовать для синтеза закон сохранения целостности объекта (ЗСЦО) [2, 4], который обеспечивает достижения цели деятельности (ЗСЦО – это устойчивая, объективная, повторяющаяся связь свойств объекта и свойств его действия при фиксированном предназначении).

Проблема 2. ЛПР решает задачи на основе модели. Для этого необходимо уметь синтезировать адекватные модели. Известны три подхода к оцениванию адекватности. Проверка на практике. Сравнение с эталоном. Полнотой учета основных закономерностей предметной области. Для решения задач ИВ подходит третий подход. Но для его реализации необходимо знать такой закон. В известных публикациях такой закон не рассматривался. Автор предлагает оценивать адекватности модели на основе ЗСЦО.

Метод решения. В процессе ИВ ЛПР работает с двумя группами систем. Это социальная и экономическая системы (1) и технико-технологическая система (2). В связи с этим методология решения задач ИВ имеет два направления применения (рис. 1). На эти две сферы деятельности воздействуют три группы факторов (3): социальных, экономических, технических.

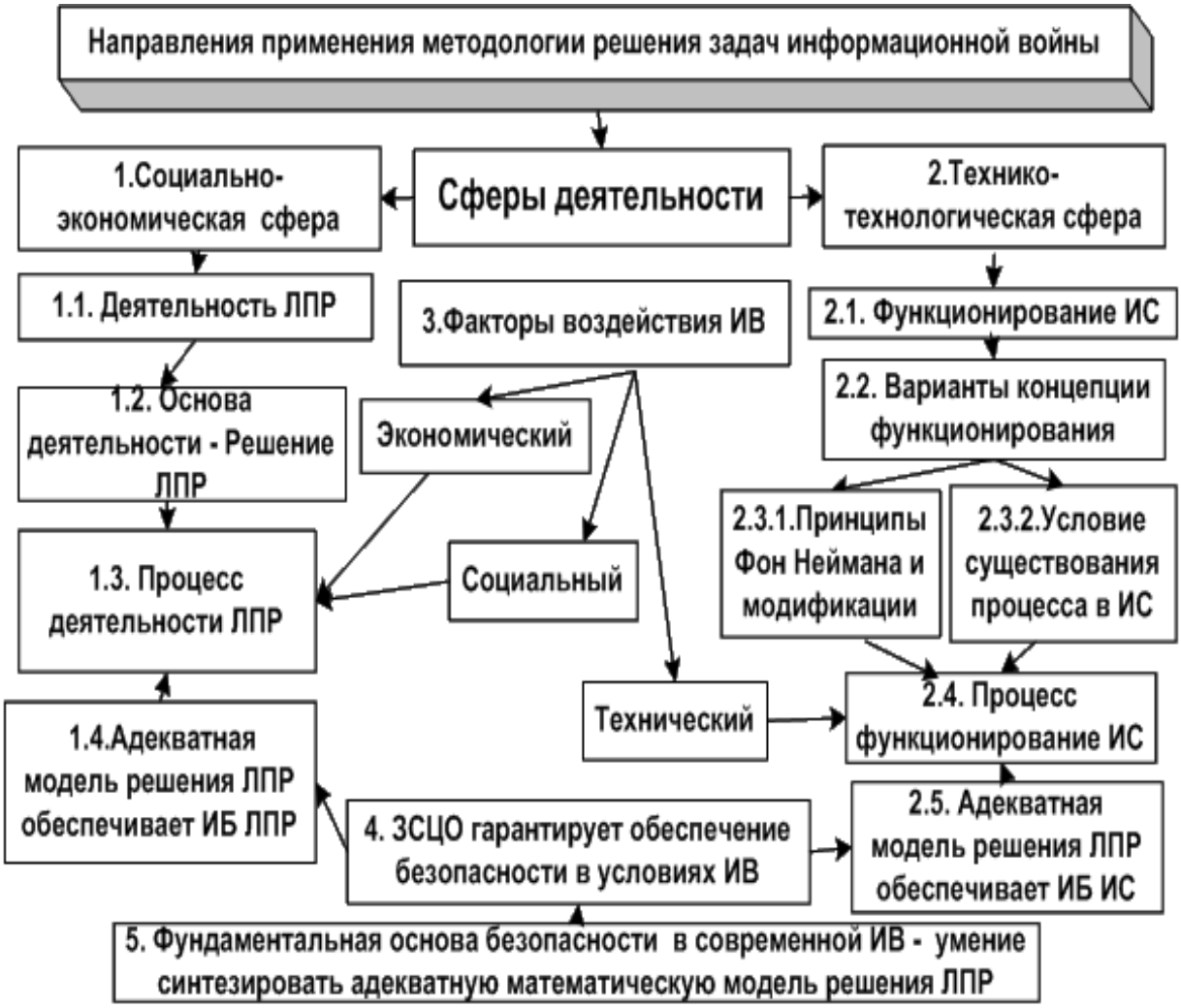


Рис. 1. Структурная схема применения методологии решения задач ИВ

Первое направление (Социально-экономическая сфера). Синтез формирования адекватных моделей социального поведения как отдельного человека, так государства в целом. Это следует из следующего. Основа деятельности – решение. Решение – это условие реализации предназначения объекта управления или самоуправления. Деятельность реализуется через управление. Предназначение ИВ – разрушение процесса управления, самоуправления человеком. Это осуществляется через разрушение модели решения. Критерием разрушения является критерий адекватности модели решения. Противостояние в ИВ осуществляют две стороны – А и Б. Задачи участников ИВ – это взаимное разрушение (сохранение адекватности) моделей решения в интересах достижения цели своей деятельности. Задача ЛПР «А» – разрушить модель решения ЛПР « Б «. Задача ЛПР « Б « – сохранить адекватность модели своего решения. И наоборот. Если модель решения ЛПР адекватна ситуации, то угрозы ИВ не актуальны. Применение ЗСЦО для синтеза модели решения ЛПР позволяет гарантировать адекватность решения ЛПР. Поэтому фундаментальной основой безо-

пасности в современной ИВ является умение синтезировать адекватную математическую модель решения ЛПР.

Второе направление (Технико-технологическая сфера). Синтез адекватной модели процесса вычислений в компьютерах и телекоммуникационных системах (информационной системе). Второе направление деятельности получило название «Обеспечение информационной безопасности» (ИБ). Это следует из следующего. Основа деятельности при обеспечении ИБ – это сохранения предназначения процесса функционирования информационной системы (ИС). Задача злоумышленника – разрушить процесс функционирования в ИС в интересах достижения цели его деятельности. Если модель процесса в ИС адекватна программно-аппаратной среде, то процесс сохраняет свое предназначение. В основу концепции построения и функционирования ИС должно быть положено условие существования процесса. В настоящее время в ИС реализованы принципы фон Неймана и их модификации. Такая модель построения и функционирования ИС не адекватна программно-аппаратной среде. Это приводит к необходимости решения комплекса задач обеспечения ИБ. ИБ при такой концепции обеспечивается ЛПР. Это требует синтеза модели решения ЛПР. Синтез позволяет осуществить ЗСЦО.

Альтернативный путь – это создание ИС с моделью, адекватной программно-аппаратной среде. Построение такой ИС требует знания закона построения и функционирования системы. Для этого целесообразно использовать ЗСЦО [2, 4, 5]. Для решения указанных проблем, методология решения задач ИВ должна давать ЛПР условие существования процесса деятельности. Решение основано на системной интеграции свойств мышления человека, свойств объектов окружающего мира и всеобщей связи явлений [4]. Человек осуществляет свою деятельность на основе модели. Поэтому для осуществления деятельности, адекватной обстановке, необходимо располагать адекватной математической моделью решения человека. Сложилась интересная ситуация – в публикациях по выработке управленческого решения утверждается, что построить математическую модель решения человека весьма проблематично, если не сказать, что нельзя. А в публикациях представлены только результаты обоснования решения, но не модель самого решения! Но без математической модели решения весьма сложно гарантировать достижения цели. Такая же ситуация и с построением системы. Отсутствует критерий правильно построенной системы.

В связи с изложенным, следует отметить следующее.

1. Для успешного решения задач ИВ необходимо уметь разрабатывать адекватную модель сложной системы и синтезировать правильно построенную сложную систему.

2. Для разработки адекватной модели сложной системы необходимо иметь формализованный критерий адекватности.

3. Для разработки правильно построенной системы необходимо знать закон построения и функционирования системы.

4. Установлено, что для успешного решения задач ИВ необходимо использовать закон сохранения целостности объекта [2–5].

Библиографический список

1. Анохин П. К. Системные механизмы высшей нервной деятельности. – М. : Наука, 1979. – 453 с.

2. Бурлов В. Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы). – СПб. : Факультет комплексной безопасности, СПБГПУ. 2007. – 265 с.

3. Бурлов В. Г. Математические методы моделирования в экономике. Часть 1. – СПб. : СПбГПУ, Факультет безопасности, НП «Стратегия будущего», 2007. – 330с.

4. Бурлов В. Г. О концепции гарантированного управления устойчивым развитием арктической зоны на основе решения обратной задачи // Информационные технологии и системы: управление, экономика, транспорт, право. – 2015. – № 2 (16). – С. 99–111.

5. Burlov V. G., Lepeshkin O.M. Modeling of process control system security based movement potentially active elements of space and time // Transportation Research Procedia. 20 (2017). pp. 100-106.

А. В. Долбилов[1]

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Несмотря на тенденцию к снижению общего количества совершенных преступлений в России, на протяжении последних нескольких лет положительную динамику показывают так называемые «киберпреступления». В связи с чем в 2017 г. Министерство внутренних дел Российской Федерации в статистическую отчетность о состоянии преступности в России добавило показатель, характеризующий количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. За январь-ноябрь 2017 г. было зарегистрировано 82 440 таких преступлений.

Одной из наиболее привлекательных для киберпреступности сфер является банковская система России.

Понятия «киберпреступление» и «киберпреступность» за последние несколько лет все чаще стали встречаться в новостных лентах российских средств массовой информации, выступлениях представителей правоохранительных органов, руководителей крупных российских банков. На сегодняшний день киберпреступления и киберпреступность стали реальной угрозой стабильности российской банковской системы.

В последние несколько лет кибератаки на российские банки носят все более целевой и организованный характер. Лица, вовлечение в кибератаки на российские банки, объединяются в преступные кибергруппы в целях разработки новых технологий и способов преодоления систем защиты безопасности банков для осуществления целевой кибератаки. Необходимо сказать и о наличии криминальной инфраструктуры для киберпреступности в банковской системе.

Высокая активность киберпреступности в банковской системе России связана с масштабным внедрением и дальнейшим развитием технологий дистанционного банковского обслуживания отечественными банками. При этом в настоящее время количество клиентов банков, которые не только интересуются, но и переходят на использование банковских услуг с применением технологий дистанционного банковского обслуживания, растет довольно высокими темпами.

---

[1] Заместитель начальника кафедры экономической безопасности, финансов и экономического анализа МосУ МВД России имени В.Я. Кикотя кандидат экономических наук. © Долбилов А. В., 2018.

Под дистанционным банковским обслуживанием в настоящее время принято понимать определенные технологии по предоставлению кредитными организациями своих услуг по передаваемым с помощью удаленных каналов банковского обслуживания распоряжениям клиентов (т. е. без визита клиента в подразделение банка), с использованием различных каналов телекоммуникации.

В качестве каналов связи могут использоваться телефонная и мобильная связь, связь посредством локальных сетей либо сети «Интернет», а также технические устройства (банкоматы и платежные терминалы). В целом дистанционное банковское обслуживание является выгодной и удобной формой взаимодействия не только для клиентов банка, но и для самого банка.

Технологии дистанционного банковского обслуживания позволяют клиенту банка осуществлять удаленное управление собственным банковским счетом. Использование дистанционного банковского обслуживания для клиентов банка позволяет осуществлять широкий спектр банковских услуг посредством удаленного доступа: возможность формирования клиентом банка платежных поручений, заявлений на перевод, покупку и продажу валюты и других операций [5].

В зависимости от выбранного канала связи принято выделять следующие формы дистанционного банковского обслуживания:

1. Классический «Банк-Клиент». 2. Интернет-банкинг. 3. Мобильный банкинг. 4. Внешние сервисы.

Сегодняшние реалии таковы, что банки предлагают все более удобные и доступные в использовании сервисы дистанционного банковского обслуживания (интернет и мобильный банкинг), которые пользуются высоким спросом среди клиентов банков. Однако из-за высокой финансовой привлекательности параллельно с технологическим развитием сервисов дистанционного банковского обслуживания к этому виду услуг растет интерес злоумышленников. В современном мире более половины всех преступлений в банковской сфере приходится на кибератаки и мошенничество в сфере дистанционного банковского обслуживания [1].

К основным угрозам кибербезопасности в банковской сфере в настоящее время можно отнести:

1) социальную инженерию;

2) несанкционированный доступ к данным и кражу идентификационной информации клиента с использованием вредоносного программного обеспечения, фишинга и других видов кибератак.

На сегодняшний день количество кибератак на российские банки во много раз превышает другие виды преступлений, совершаемых в банковской сфере, в связи с чем и имущественный ущерб от киберпреступлений намного выше, чем от других видов преступлений. При этом правоохранительная система обладает ограниченным количеством специалистов, которые могут заниматься выявлением и расследованием киберпреступлений, производством необходимых экспертиз [2].

Особенность киберпреступности также заключается и в отсутствии государственных границ для совершения киберпреступлений, в связи с чем преступные кибергруппы имеют возможность совершать кибератаки на российские банки, находясь в любой точке мира [3, 4].

Все перечисленные факторы в совокупности являются той причиной, почему российские банки являются наиболее лакомым куском для совершения кибератак.

Для снижения уровня киберугроз в банковской сфере и минимизации ущерба от кибератак необходим комплекс мер, заключающийся в совершенствовании уголовного законодательства, объединении сил и средств банков и правоохранительных органов для противодействия киберпреступности в банковской сфере, подготовка в правоохранительных органах специалистов, которые могут заниматься выявлением и расследованием киберпреступлений, производством необходимых экспертиз.

Библиографический список

1. Иванов В. Ю. Использование особенностей операционной системы Windows для поиска следов, связанных с загрузкой файлов в ходе компьютерного инцидента // Технологии информационной безопасности в деятельности ОВД. – М. : МосУ МВД России, 2016. – С. 154–156.

2. Береснев Д. С., Иванов В. Ю. Исследование логов при расследовании компьютерных преступлений // Технологии информационной безопасности в деятельности ОВД. – М. : МосУ МВД России, 2016. – С. 58–61.

3. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации : сб. научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

4. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (т. 2).

5. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – Т. 2. – № 2 (20). – С. 30–38.

С. И. Козьминых[1]

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРРОРИЗМУ

Стремительное развитие информационных технологий и процессов глобализации в конце XX и начале XXI в. привело к тому, что на смену традиционным силовым методам ведения войны пришли информационные войны [1]. Каждый день мы встречаемся с огромным потоком новостей, которые различные средства массовой информации подают под определенным углом, факты часто искажаются, и обычному обывателю становится все сложнее и сложнее выявить, где истина, а где ложь. В наше время только специалисты аналитики могут объективно оценивать, где пропаганда, а где реальные факты, которые представляются мировыми изданиями, в телепрограммах и в интернет-новостях. Рассматривая опыт использования различными странами информационного воздействия на противника в период различных региональных конфликтов и гражданских войн, можно с уверенностью сказать, что в настоящее время именно информационное противоборство становится главным оружием, которое во многом определяет победу или поражение той или иной стороны.

Сущность и содержание информационного противоборства. Технологии ведения информационных войн появились задолго до возникновения современных конфликтов. Получение и манипулирование информацией для достижения политических и военных целей использовалось еще, когда появились первые государства. Поиск и добывание необходимой, особой важной информации были одной из главных задач. Добытая информация эффективно использовалась государственными и военными деятелями Вавилона, Китая, Древнего Рима и Греции [2].

Сегодня секреты производства шелка уже мало кого интересуют, более актуальны секреты, связанные с инновационными технологиями, базами данных, банковскими счетами и личной конфиденциальной информацией. В качестве примера современного шпионажа следует напомнить, как был задержан сотрудниками ФСБ России по Свердловской области в феврале 2015 г. гражданин Украины, который

---

[1] Профессор кафедры информационной безопасности Финансового университета при Правительстве Российской Федерации доктор технических наук.
© Козьминых С. И., 2018.

занимался сбором научно-технической информации о деятельности российских машиностроительных предприятий.

Еще одним ярким примером информационного противодействия является операция, разработанная США и их союзниками, направленная против Ирака. Основой этой операции была развернутая пропаганда о наличии в Ираке химического оружия, угрожающего всему миру. В результате этой пропаганды в Ирак были введены войска американской коалиции, развязана война, свергнуто законное правительство, казнен руководитель государства и страна ввергнута в полный хаос. При этом химического оружия так и не было обнаружено. Власть в стране захватили радикальные исламисты, которые в настоящее время бесчинствуют на территории Ирака, воюют в Сирии, а также совершают террористические акты по всему миру.

Антиконституционному перевороту в Украине также предшествовала длительная информационная обработка (пропаганда) как своего населения страны, так и мирового сообщества, нацеленная на создание отрицательного облика России, якобы виновной во всех бедах Украины. Результатом такой обработки явились незаконный захват власти, раскол страны, гражданская война, глубокий экономический кризис, разорение народа Украины и разрыв связей с Российской Федерацией [3].

Таким образом, в настоящее время можно отметить возрастание интенсивности информационного противоборства, в первую очередь связанного с различными политическими конфликтами. Усиление информационного противоборства, с одной стороны, спровоцировано обострением политической ситуации в мире, а с другой – связано со значительной модернизацией информационной глобальной инфраструктуры, которая используется для достижения политических, экономических и других целей.

В результате анализа научной литературы можно сделать вывод, что информационное противоборство включает в себя классические методы борьбы такие, как: физическое воздействие на линии передачи информации, прямое изъятие информации и другие ранее известные методы. А также новые методы борьбы, такие как: киберпреступность и кибертерроризм, включая компьютерные атаки, взлом компьютерных данных, подмену информации в информационных хранилищах, и другие методы. Некоторые исследователи полагают, что информационная война вступает в эпоху, так называемых бескровных конфликтов, противостояние происходит в киберпространстве. И «кибервои-

ны» или так называемые хакеры имеют гораздо большее значение, чем отдельные вида вооружений [4].

Вместе с развитием и распространением новых информационных технологий, возникают все новые и новые формы атак, которые качественно отличаются от прежних. Использование таких инструментов, как компьютерный взлом или внедрение вредоносных компьютерных программ, может перенести войну из реального физического мира в нематериальный виртуальный мир. Для современных хакеров не существует границ. Компьютерные атаки могут быть реализованы на большом расстоянии посредством использования радиосвязи или через сети проводной международной связи, без физического вмешательства и за пределами территориальных границ страны-противника. Ущерб противнику может быть причинен различный, например, это может быть причинение физического ущерба военным или гражданским лицам либо сбои в работе компьютерных систем, отказ работы важных военных или правительственных систем связи в момент устранения кризиса в стране [5]. Все это может привести к созданию экономических трудностей или просто к нарушению нормальных условий жизни населения, которые зависят от работоспособности различных информационных систем.

В качестве примера можно напомнить инцидент, когда для россиян были заблокированы операции в зарубежных платежных терминалах с международными пластиковыми картами Viza и MasterCard. В результате в России пришлось срочно создавать свою международную платежную систему «Мир», которая надежно защищена от внешних угроз.

Каждую секунду десятки человек становятся жертвами какого-либо кибермошенничества. Причем наиболее вероятными жертвами становятся молодые люди, которые выходят в «Интернет» через мобильные телефоны.

Вирус Wanna Cry наделал много шума 12 мая 2017 г. Этот вымогатель и шифровальщик буквально парализовал работу структур и ведомств в 73 странах мира. Специалисты не могли попасть в базы данных на своих ПК, т. к. на экране монитора высвечивалось единственное сообщение о том, куда и сколько надобно перевести денег в биткоинах.

Bad Rabbit (рус. «Плохой кролик») – вирус шифровальщик, разработанный для ОС семейства Windows и обнаруженный 24 октября 2017 г., атаковал ряд российских СМИ, включая ИА «Интерфакс» и

интернет-газету «Фонтанка», а также киевское метро и аэропорт Одесса, требуя за разблокировку одного компьютера 0,05 биткоинов (около 16 тыс. руб.) в течение 48 часов. Также, в меньшей степени, атаке подверглись Турция и Германия. Восстановление работы сайта и компьютеров «Интерфакса» заняло более суток.

Следует отметить, что для таких массированных атак, которые осуществлялись с помощью указанных вирусов шифровальщиков, необходимы значительные силы и средства. А целью этих атак явно было неполучение какой-либо экономической выгоды, а совершение акта кибертерроризма в целях дестабилизации деятельности отдельных средств массовой информации, транспортных объектов и в конечном счете, политического давления на государства.

Приведенные примеры только лишний раз доказывают, что мы уже вступили в эпоху кибервойн, которые могут причинять ущерб воюющим сторонам не меньший, чем традиционные войны.

В настоящее время возникает проблема трактовки и определения «информационной войны». Наиболее близким в международной практике является определение «агрессии», которое дано в резолюции 3314 Генеральной Ассамблеи ООН и Декларации по агрессии. Там агрессия определяется как «применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства или каким-либо другим образом, несовместимым с Уставом Организации Объединенные Нации».

По степени ущерба последствия агрессии могут быть сравнимы с последствиями информационных войн. Следовательно, в международной практике ведение информационных войн может быть приравнено к агрессии одного государства в отношении другого или других.

Сложность трактовки некоторых форм информационной войны как «применение силы» или «агрессия» в рамках международного права не означает, что международно-правовые институты не могут ответить на подобные вопросы. Например, глава VII Устава ООН дает Совету Безопасности ООН полномочия на определение наличия каких-либо угроз миру или актов агрессии, и Совет Безопасности ООН в таких случаях может рекомендовать какие-либо меры противодействия. Многие информационные атаки, которые не могут представлять собой по определению «применение силы» или «агрессию», безусловно, можно трактовать как угрозу миру и, следовательно, они подлежат рассмотрению в Совете Безопасности [6]. Тем не менее, в связи со

сложностью процедуры принятия резолюций в Совете Безопасности ООН, в том числе связанной с правом вето, реакции на подобные действия могут быть не столь оперативны, насколько этого требует какая-либо конкретная ситуация.

Безусловно, информационные войны имели место в истории на протяжении всего существования человечества, и с каждым столетием они становятся все более изощренными. Информационное противоборство на современном этапе истории человечества характеризуется более сложными методами воздействия одного государства (сообщества) на другое. В борьбе за природные ресурсы и территории появились новые методы войны – не физические, а стратегические и тактические, это – информационное противоборство.

Основные направления совершенствования деятельности в области противодействия киберпреступности и кибертерроризму. В XXI в. Российская Федерация вступила с определенным набором инструментов обеспечения безопасности нашей страны. Но в связи с тем, что инструменты ведения информационных войн в настоящее время значительно усовершенствовались, появилась необходимость совершенствования и защитных механизмов в ответ на информационные вызовы [1]. Как показал конфликт в Южной Осетии, наша страна, к сожалению, не смогла эффективно противостоять информационным технологиям западных СМИ, вследствие чего в течение достаточно длительного времени в мировом сообществе существовал негативный образ России. Смонтированные и отретушированные видеоматериалы новостей ведущих телевизионных каналов мира об «агрессивных действиях» российских войск в зоне действия грузино-осетинского конфликта, «огромных жертвах среди грузинских мирных жителей» формировали определенное сочувствие у мирового сообщества по отношению к Грузии и, с другой стороны, негативное отношение к миротворцам России. В данный момент противовесом западных СМИ является телевизионный российский канал Russia Today, который постоянно подвергается нападкам со стороны запада. Однако поскольку он один, а их много, он не может эффективно противостоять западным СМИ.

Одной из главных задач нашего государства в настоящее время является необходимость соотношения и разделения таких понятий, как «агрессия» и «информационная атака», а также других понятий в этой области в целях внесения их в международное право. Российская Федерация может быть инициатором в этой сфере для того, чтобы в

дальнейшем использовать внесенные изменения для разрешения международных споров и пользоваться «правом самообороны» в ответ на информационные атаки.

Использование понятия «информационная атака» в международном праве может дать основу для «маневрирования» в юридических спорах и повысить эффективность политических и дипломатических действий в отношении вышеуказанных атак. Преследуя цель защиты гражданского населения во время информационной войны, Россия могла бы заранее заключить международные договоры, которые будут способствовать снижению не только политического ущерба страны, но и материального ущерба, вызванного определенными видами информационных атак. Россия могла бы повлиять на развитие международного права в сфере борьбы с информационными войнами через декларации Генеральной Ассамблеи ООН [7]. Тогда атака на информационные системы Российской Федерации будет попадать под законодательную юрисдикцию России, несмотря на то, что исполнители могут быть вне досягаемости государственных служб России. В случае компьютерного нападения Российская Федерация может оправдать ответные действия, направленные на прекращение атаки или предотвращение атак, с помощью ст. 51 Устава, предусматривающей право на самооборону. Однако данное основание может быть спорным в случае проведения военных действий против другого государства, проводившего информационные атаки.

Как уже говорилось выше, мирное урегулирование споров является одним из основных принципов Устава Организации Объединенных Наций. Устав запрещает угрозу силой или применение силы одним государством против территориальной целостности или политической независимости другого государства. Единственным легитимным применением силы можно считать коллективные действия по принуждению к миру под эгидой ООН либо индивидуальную или коллективную самооборону против вооруженного нападения. Интернет-атака на компьютеры или атака с использованием инструментов информационной войны, таких как вирусы, является спорным определением вооруженного нападения, которые, безусловно, необходимо закрепить в международном праве.

Вторая задача заключается в том, что Российская Федерация должна развивать международное сотрудничество в сфере противодействия киберпреступности и кибертерроризму.

В связи с этим России необходимо укреплять международные связи в этой сфере путем гармонизации законов и сотрудничества в расследовании и уголовном преследовании преступников, совершающих преступления с использованием современных информационных технологий. Решение этой задачи должно включать в себя дипломатическое взаимодействие и консультации по уголовному правосудию в сфере информационных атак, а также содействие в закреплении понятия «информационные атаки» в качестве противоправных действий в тех странах, которые еще не признают таких атак в качестве преступлений. Кроме того, необходимо предусмотреть разработку процедуры выдачи преступников, совершающих компьютерные атаки, предполагающую обязательную их экстрадицию в страну, против которой эта атака была совершена.

Не менее важной задачей в области обеспечения безопасности Российской Федерации должна быть защита критически важных информационных систем не только от информационных атак, но и от террористических угроз, локальных и глобальных войн и стихийных бедствий. Некоторые информационные системы могут быть настолько критически важными, что большинство стран будут заинтересованы в сотрудничестве в целях их защиты. Предметом такой защиты могут быть объекты атомной энергетики, электронные международные финансовые рынки, банки, биржи, центры связи, информационные системы железнодорожного транспорта, авиасообщений и медицинские базы данных.

Политика России в области информационного противодействия должна включать два основных направления, первое должно обеспечить надежную защиту всех информационных ресурсов России, а второе – это активное участие в информационном противодействии враждебным средствам массовой информации, искажающим факты и формирующим отрицательный облик нашей страны в глазах мирового сообщества.

Для решения первой задачи необходимо определить, какие информационные ресурсы России представляют наибольший интерес для потенциальных противников и наибольшую ценность для правоохранительной деятельности. Необходимо определить величину рисков для этих ресурсов, исходя из вероятности угроз, которые могут на них воздействовать, величину ущерба, который может быть причинен этим ресурсам, и эффективность мер защиты. Чем более эффективные

меры будут использоваться для защиты информационных ресурсов, тем меньше риски их потерять.

Для решения второй задачи необходимо активизировать работу по выявлению легальных и не легальных организаций, работающих на враждебные средства массовой информации, финансируемые иностранными разведками и осуществляющие подрывную информационную деятельность. Ликвидация таких организаций, широкое освещение их подрывной деятельности и привлечение их к законной ответственности позволят значительно снизить риски информационного воздействия, направленного протии Российской Федерации.

Достаточно сложно определить, какой именно урон наносится стране в период ведения информационной войны. Зачастую общество не подозревает о том, что на него воздействуют с определенным умыслом. В результате получается «обработанное» общество, которое восстает против законно избранной власти.

В качестве вывода следует отметить, что основные инструменты урегулирования информационных войн и противодействия киберпреступности и кибертерроризму в правовом поле уже существуют. К ним относятся: нормативные правовые акты Международного союза электросвязи, Международное космическое право, нормативные правовые акты Международного гуманитарного права. Несмотря на уже существующую правовую базу, следует констатировать, что на данный момент, ее пока не хватает. Многие страны находятся в зоне риска киберпреступности и кибертерроризма, в том числе и наша страна. Конфликты переходят из реального мира в виртуальный, однако ущерб может оказаться не только виртуальным, но и материальным. Мы должны учитывать ошибки прошлого, чтобы не совершать их в будущем.

Библиографический список

1. Степанов О. А., Баранов В. В., Клементьев А. С., Некишев А. В., Шмонин А. В. Актуальные проблемы противодействия преступлений в сфере высоких технологий / под ред. О. А. Степанова. – М. : Академия управления МВД России, 2013.

2. Овчинский А. С. Информационные воздействия и организованная преступность: курс лекций. – М. : ИНФА-М, 2007.

3. Козьминых С. И. Организация защиты информации в российской полиции: учебное пособие. – М. : ЮНИТИ-ДАНА: 2016.

4. Андрианов В. В., Зефиров С. Л., Голованов В. Б., Колдуев Н. А. Обеспечение информационной безопасности бизнеса / 2-е изд. перераб. и доп. – М. : Альпина Паблишерз, 2011.

5. Барабанов М. В., Денисенцев С. А., Кашин В. Б. и др. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего. – М.: Центр анализа стратегий и технологий, 2015.

6. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб. : Питер, 2008.

7. Уин Швартау. На пороге мировой информационной войны. – Network World, США. 09, 2007.

***Д. В. Милютин*[1], *Д. А. Панин*[2]**

СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА: УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИЛИ НОВЫЙ ЭТАП В РАЗВИТИИ ВЫСОКИХ ТЕХНОЛОГИЙ

В последние время в средствах массовой информации и юридической литературе все чаще обсуждаются вопросы законности и правомерности привлечения к уголовной ответственности лиц, приобретающих и использующих специальные технические средства. Высокая заинтересованность по данному вопросу обусловлена тем, что по всей России ежегодно возбуждаются сотни уголовных дел за попытки купить детские игрушки с видеокамерой, наручные часы с микрофоном, очки с возможностью видеофиксации и др. Такие устройства зачастую используются в личных интересах в целях безопасности членов семьи и сохранности своего имущества. По данным МВД России, только за шесть месяцев 2017 г. выявлено 311 преступлений по ст. 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», их них 168 дел (54 %) направлено в суд с обвинительным заключением (рис).

Стоит отметить, что в настоящее время нет однозначной трактовки понятия «специальные технические средства». По мнению В. Т. Батычко, к ним относятся любые технические средства и приспособления, не причиняющие вреда жизни и здоровью личности и используемые для получения информации о переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях граждан [1]. Другие авторы полагают, что это технические средства, предназначенные (разработанные, приспособленные, запрограммированные) прежде всего для негласного получения информации [2].

---

[1] Старший научный сотрудник ФГКУ «Всероссийского научно-исследовательского института МВД России». © Милютин Д. В., 2018.

[2] Старший научный сотрудник ФГКУ «Всероссийского научно-исследовательского института МВД России» кандидат экономических наук. © Панин Д. А., 2018.

Рис. Количество преступлений по ст. 138.1 УК РФ за 2012–2017 гг.

В Постановлении Правительства Российской Федерации от 10.03.2000 г. №214 обозначены критерии, которым должны отвечать специальные технические средства, в частности, выделены такие критерии, как закамуфлированность, малогабаритность, наличие специальных технических параметров и др.

Мы придерживаемся мнения В. В. Гирийчука, который считает, что специальные технические средства – это совокупность технических устройств и приспособлений, ограниченных в обороте, предназначенных (разработанных, приспособленных, запрограммированных) для контролируемого, негласного получения информации оперативными подразделениями органов внутренних дел при проведении оперативно-разыскных мероприятий в целях решения задач оперативно-разыскной деятельности [3].

В настоящее время действующее законодательство четко определило круг субъектов, имеющих право на использование специальных технических средств. Так, Федеральный закон «Об оперативно-разыскной деятельности» в их число отнес должностных лиц, уполномоченных на осуществление оперативно-разыскной деятельности, при наличии соответствующих оснований и условий в пределах, предоставленных им полномочий. Однако, как показывает практика, данные средства применяются не только должностными лицами правоохранительных структур, но и частными коммерческими организациями и физическими лицами.

Если правомерность использования специальных технических средств правоохранительными органами не вызывает сомнений, то использование их лицами, не наделенными правами осуществлять оперативно-разыскную деятельность и в целях получения преимуществ перед другими гражданами, недопустимо и посягает на основополагающие институты гражданского общества. Именно по этой причине законодатель определил меры уголовно-правового характера за незаконное производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, а именно ст. 138.1 УК РФ.

Несмотря на это, в правоприменительной практике по данному вопросу существуют серьезные проблемы, основной из которых является «неторопливость» правовой системы. Это выражается в несвоевременном реагировании органов исполнительной и законодательной власти на изменения, происходящие в обществе, такие как развитие технического прогресса и последующее за ним внедрение в повседневную жизнь его результатов в виде технических приспособлений с новыми функциональными возможностями.

Стоит отметить, что последние изменения в Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 датированы 2002 г. и относились только к «части утверждения Положения о лицензировании [4]», не затрагивая сам перечень и критерии специальных технических средств. То есть технические возможности устройств, которые позволили отнести его к специальным техническим средствам, предназначенным для негласного получения информации, определены на основании возможностей имевших место двадцать два года назад. Постановление Правительства Российской Федерации от 01 июля 1996 г. № 770 определяет следующие технические возможности оборудования, позволяющего отнести его к специальным техническим средствам, а именно:

– негласное получение и регистрация акустической информации;

– негласное визуальное наблюдение и документирование;

– негласный контроль за перемещением транспортных средств и других объектов;

– негласная идентификация личности.

Также ряд других признаков, таких как камуфлированность под бытовые предметы, малогабаритность и т. д., определен в Постановлении Правительства Российской Федерации от 10 марта 2000 г. № 214 в списке видов специальных технических средств, предназна-

ченных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию.

Именно в данной квалификации в полной мере и проступает обозначенная проблема, поскольку на момент определения данных категорий в 1996 г. они были актуальны и позволяли реально квалифицировать оборудование как специальные технические средства. Однако в настоящее время указанным функционалом обладает практически любой мобильный телефон. Так, например, большинство из них позволяет негласно осуществлять видеосъемку и аудиозапись, отслеживать перемещение различных объектов возможно с помощью GPS-маяков, идентифицировать личность по изображению или речи. Малогабаритность сегодня можно отнести к архаичным признакам, т. к. с момента его нормативно-правового закрепления средние размеры технических средств уменьшились на несколько порядков.

К примеру, в 2017 г. известная компания выпустила самый маленький в мире телефон Zanco Tiny T1, обладающий полным функционалом мобильного телефона, а также возможностями фиксации аудиоинформации, определения местоположения. Данное устройство имеет габариты 46,7х21х12 мм и вес 12 г при возможности автономной работы в течение трое суток. Можно с уверенностью сказать, что в 1996 г. указанные габариты соответствовали, например, элементу питания, являющимся всего лишь составной частью оборудования, обладающего значительно меньшим функционалом.

Критерий маскировки под бытовые приборы в настоящее время необходимо рассматривать индивидуально для каждого случая, т. к. «джентльменским» набором в виде возможности видеозаписи, аудиозаписи, удаленного управления функциями обладает довольно широкий спектр бытовых приборов. Данные возможности изначально конструктивно заложены производителем, описаны в сопутствующей документации, широко освещены в рекламной продукции. На наш взгляд, критерий маскировки необходимо принимать во внимание только в случае, если конструктивные особенности оборудования не предусматривают наличия возможности видеозаписи, аудиозаписи, контроля за перемещением объектов и т. д., либо оно наделено данной функцией, но она намеренно скрыта для его возможного негласного использования.

Учитывая описанную проблематику, можно привести два ярких примера иллюстрирующих проблемы правоприменительной практики.

В 2016 г. в городе Серпухов Московской области супруги «М» были привлечены к уголовной ответственности по ст. 138.1 УК РФ. Так, в ходе проведения оперативно-разыскных мероприятий у гражданки М был закуплен офисный калькулятор, оборудованный устройством фиксации и аудиоинформации с возможностью ее удаленной передачи по GSM-каналу. При проведении негласной проверочной закупки гражданка «М» пояснила, что данное оборудование предназначено для негласного получения аудиоинформации, прослушивать которую можно посредством мобильного телефона, надлежащим образом подключенного к GSM-модулю, установленному в калькуляторе. С целью противодействия правоохранительным органам гражданкой М при реализации с покупателем был заключен договор аренды данного оборудования сроком на 99 лет. Как она пояснила, данное действие необходимо для того, чтобы избежать уголовной ответственности, т.к. якобы в этом случае деяние не будет попадать под категорию распространения. После осуществления негласной проверочной закупки приобретенное оборудование было направлено на проведение исследования, по результатам которого оно было признано специальным техническим средством, предназначенным для негласного получения информации. По результатам проведенных оперативно-разыскных мероприятий СО по г. Серпухов ГСУ СК РФ по Московской области было возбуждено уголовное дело по факту преступления, предусмотренного ст. 138.1 УК РФ. В ходе предварительного следствия по месту жительства супругов М бы проведен обыск, в ходе обыска было обнаружено порядка двухсот единиц оборудования, предназначенного для негласного получения информации, в виде различных бытовых приборов, предметов одежды и т. д. В доме была обнаружена радиомастерская, в которой гражданином М осуществлялся ремонт и сборка специальных технических средств, предназначенных для негласного получения информации. В дальнейшем по результатам проведенной экспертизы обнаруженное оборудование было признано специальным техническим средством, предназначенным для негласного получения информации. По данным фактам супруги М пояснили, что указанное оборудование они закупают в Китае и перепродают на территории Москвы и Московской области. По результатам рассмотрения материалов проведенного расследования Серпуховским городским судом Московской области в отношении супругов М был вынесен обвинительный приговор по ст. 138.1 УК.

В 2017 году на территории Курганской области в отношении гражданина «В» возбужденно уголовное дело по признакам состава преступления предусмотренного ст. 138.1 УК РФ, чему предшествовало следующее. Гражданином В. в зарубежном интернет-магазине был осуществлен заказ портативного устройства, обладающего функциями фиксации аудиоинформации с возможностью ее удаленной передачи по GSM-каналу и контроля за перемещением объектов. Пересылаемое устройство было обнаружено сотрудниками таможенной службы, о чем было сообщено в территориальные правоохранительные органы. При получении почтового отправления, содержащего указанное устройство гражданин В был задержан сотрудниками ФСБ. Из его показаний следовало, что данное оборудование приобреталось им с целью отслеживания передвижения имеющегося у него крупнорогатого скота. По результатам проведенной проверки в отношении гражданина В возбуждено уголовное дело, предусмотренное ст. 138.1 УК РФ, по окончании предварительного расследования материалы уголовного дела были направлены в Лебяжьевский районный суд Курганской области. В настоящее время в связи с широким общественным резонансом суд принял решение о возвращении уголовного дела на доследование.

Если в первом случае преступный умысел очевиден и действия лиц были направлены на производство и распространение технических средств, предназначенных для негласного получения информации, то в другом случае лицо привлекается к ответственности по формальным признакам преступления, поскольку устройство приобреталось для сохранности своего имущества. Несмотря на разную степень общественной опасности за данные деяния, в обоих случая были возбуждены уголовные дела по ст. 138.1 УК РФ «Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации».

По мнению авторов, именно то, что ст. 138.1 была внесена в гл. 19 УК РФ, содержащую преступления против конституционных прав и свобод человека и гражданина, подтверждает то, что рассматривать проблему регулирования оборота специальных технических средств, предназначенных для негласного получения информации, в отрыве от нарушения различных видов тайн нецелесообразно и контрпродуктивно.

Полагаем, что решение описанной проблемы заключается в следующем. Рассматривать проблему оборота специальных технических

средств, предназначенных для негласного получения информации в отрыве от рассматривания категорий информации, которую предполагается получить данным способом, нецелесообразно. Основным критерием информации, которую необходимо охранять от получения сторонними лицами, является личная информация гражданина, которую он не имеет желания сообщать любому иному лицу.

На наш взгляд, необходимо внести изменения, позволяющие разграничить мотивы приобретения, распространения, изготовления специальных технических средств, предназначенных для негласного получения информации.

В связи с этим полагаем изложить ст. 138.1 УК РФ в следующей редакции: «*Незаконные изготовление и приобретение специальных технических средств, предназначенных для негласного получения информации, с целью негласного получения охраняемой законом информации, либо незаконное распространение специальных технических средств, предназначенных для негласного получения информации, с целью обеспечения лицу, приобретающему данное оборудование, возможности негласного получения охраняемой законом информации – наказывается…*». В случае, если деяние, совершаемое лицом, затрагивает только круг его законных прав и не затрагивает или не позволяет в дальнейшем затронуть охраняемые законом права иных лиц, привлечение к уголовной ответственности не является обоснованным и отвечающим принципам уголовного закона.

Внести изменения в Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 и Постановление Правительства Российской Федерации от 10 марта 2000 г. № 214 в части конкретизации типовых характеристик оборудования, используемого для негласное получения информации, которые позволят исключить факты привлечения к уголовной ответственности за оборот технических средств, который не представляет общественной опасности.

Остается лишь надеяться, что законодатель как можно скорее отреагирует на описанную проблему и осуществит все необходимые действия, которые позволят исключить случаи необоснованного и несправедливого привлечения к ответственности граждан.

Библиографический список

1. Родивилина В. А. Родивилин И. П. Особенности квалификации преступлений в сфере незаконного оборота специальных технических средств, предназначенных для негласного получения информации // Вестник Восточно-Сибирского института МВД России. – 2013.

2. Специальная техника органов внутренних дел. Технические средства связи в органах внутренних дел // Уральский юридический институт МВД России http://212.49.112.154/moodle/media_book /page97.html.

3. К вопросу о понятии специальных технических средств, предназначенных для негласного получения информации, применяемых в оперативно-разыскной деятельности органов внутренних дел https: // cyberleninka.ru.

4. Постановлением Правительства Российской Федерации от 15.07.2002 г. № 526 // СПС «КонсультантПлюс».

А. В. Долбилов[1]***, О. С. Дудко***[2]

ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ КИБЕРАТАК НА БАНКИ

Целевые (APT) кибератаки стали уже настолько широко распространены, что редкая неделя обходится без сообщений о них. В Trend Micro и IDC полагают, что целенаправленные атаки станут одним из самых распространенных видов угроз в 2018 г.

APT – это сокращение от Advanced Persistent Threat, т. е. сложная постоянная угроза. Термин известен давно, но стал действительно популярен после разоблачительного материала в «Нью-Йорк таймс», где рассказывалось об атаке на эту газету, устроенной китайской военной структурой, теперь известной как APT 1. Атака также проводилась на многие корпоративные сети при помощи серии фишинговых посланий и специально написанных вредоносных программ.

Рассматривать APT можно с двух сторон: это и сама атака, и это люди, стоящие за ней. С одной стороны, сложная постоянная угроза (APT) является высокоточной кибератакой. С другой стороны, APT можно назвать группу, спонсируемую государством либо иным покровителем, оплачивающим целевую атаку.

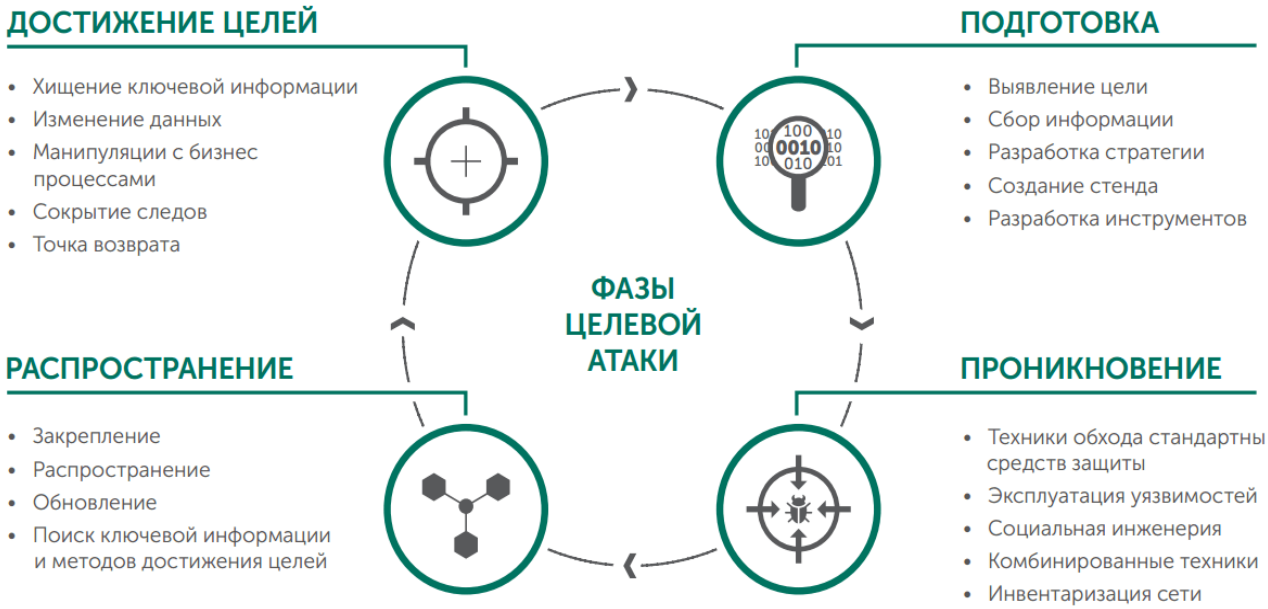
Когда речь идет о киберпреступниках и распространителях вредоносных программ, принято считать, что их целью является заражение как можно большего числа компьютеров и хищение оттуда данных либо создание на их основе бот-сети для массовой атаки. Чем шире созданная сеть, тем больше возможностей для кражи денег, мощнее

---

[1] Заместитель начальника кафедры экономической безопасности, финансов и экономического анализа МосУ МВД России имени В.Я. Кикотя кандидат экономических наук. © Долбилов А. В., 2018.

[2] Курсант 228 учебного взвода факультета подготовки сотрудников для подразделений экономической безопасности и противодействия коррупции МосУ МВД России имени В.Я. Кикотя. © Дудко О. С., 2018.

вычислительные ресурсы и серьезнее последствия. APT-атаки же направлены на заражение компьютера всего лишь нескольких конкретных людей [1, 5].



На приведенном рисунке отображены четыре фазы целевой атаки, демонстрирующие ее жизненный цикл. Кратко сформулируем основное назначение каждой из них:

1. Подготовка. Основная задача первой фазы – найти цель, собрать о ней достаточно детальной приватной информации, опираясь на которую выявить слабые места в инфраструктуре. Выстроить стратегию атаки, подобрать ранее созданные инструменты, доступные на черном рынке, либо разработать необходимые самостоятельно. Обычно планируемые шаги проникновения будут тщательно протестированы, в том числе на необнаружение стандартными средствами защиты информации.

2. Проникновение – активная фаза целевой атаки, использующая различные техники социальной инженерии и уязвимостей нулевого дня, для первичного инфицирования цели и проведения внутренней разведки. По окончании разведки и после определения принадлежности инфицированного хоста (сервер/рабочая станция) по команде злоумышленника через центр управления может загружаться дополнительный вредоносный код.

3. Распространение – фаза закрепления внутри инфраструктуры преимущественно на ключевые машины жертвы. Максимально распространяя свой контроль, при необходимости корректируя версии вредоносного кода через центры управления [3].

4. Достижение цели – ключевая фаза целевой атаки, в зависимости от выбранной стратегии в ней могут применяться: хищение закрытой информации; умышленное изменение закрытой информации; манипуляции с бизнес-процессами компании.

На всех этапах выполняется обязательное условие по сокрытию следов активности целевой атаки. При завершении атаки часто бывает, что киберпреступники создают для себя «точку возврата», позволяющую им вернуться в будущем.

Можно выделить следующие типы атак [4]:

Атака на конкретное предприятие. Целью такой атаки является проникновение в информационную систему компании. Обычно производится с помощью рассылки сообщений с вредоносными вложениями, которая направлена на всех сотрудников компании и партнеров, с которыми у компании установлены доверительные отношения. Атакованы могут быть как рядовые сотрудники, так и руководство. Такие атаки выполняются под заказ или по приказу [2].

Охота на китов (whaling). Это атака на руководство компаний в целях получения доступа к экономической или стратегической информации компании. Производится с помощью сайтов, которые посещают руководители компаний определенного сектора экономики. Часто такие атаки связаны со шпионажем или конкурентной разведкой, однако, без конкретной цели – только отрасль или отдельные сегменты.

Атака на отрасли экономики – масштабный вид атаки, нацеленный на крупные организации. Например, на Научно-исследовательские институты. Целью атак является хищение ценной информации. Как правило, подобные атаки проводятся под заказ.

Kill Chain. Кибератака изначально может быть проведена на людей никак напрямую не связанных с целевой организацией, например, на семью одного из сотрудников. В таком случае заражению подвергается сперва компьютерная система супруга или супруги (доверенного лица) сотрудника организации, далее от его/ее имени высылается ссылка на какую-либо интересную новость/фото, после чего проникновение в систему продвигается по цепочке, до достижения желаемой цели.

Библиографический список

1. Родкина Е. А., Иванов В. Ю. Некоторые аспекты мониторинга социальных сетей // Технологии информационной безопасности в деятельно-

сти органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 86–89.

2. Береснев Д. С., Иванов В. Ю. Исследование логов при расследовании компьютерных преступлений // В сборнике: Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 58–61.

3. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–6.

4. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (том 2).

5. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. . – 2017. – № 2 (том 2). – С. 30–38.

***Н. Ю. Ромашкина*[1], *А. В. Долбилов*[2]**

КИБЕРПРЕСТУПНОСТЬ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ

Как сообщает ТАСС, ссылаясь на руководителя Сбербанка России г. Грефа, за 2016 г. 98,5 % правонарушений в финансовой сфере пришлось на киберпреступления.

Греф заявил, что количество киберпреступлений составляет миллионы, а к ответственности привлечено гораздо меньшее число виновных. Он отметил, что причиной этому являются несовершенная нормативно-правовая база, а также дефицит специалистов в сфере борьбы с киберпреступностью. Глава Сбербанка также отметил, что настоящие методы борьбы с этим антиобщественным явлением просто «трата времени и денег», в то время как мировые потери от киберпреступности в 2015 г. составили 500 млрд долларов (4 млрд долларов в России) [1].

Самым распространенным из способов совершения киберпреступлений в финансово-кредитной сфере является использование вредоносных программ с помощью системы интернет-банкинга [5, 6].

---

[1] Курсант 228 учебного взвода факультета подготовки сотрудников для подразделений экономической безопасности и противодействия коррупции МосУ МВД России имени В.Я. Кикотя. © Ромашкина Н. Ю., 2018.

[2] Заместитель начальника кафедры экономической безопасности, финансов и экономического анализа МосУ МВД России имени В.Я. Кикотя кандидат экономических наук. © Долбилов А. В., 2018.

Интернет-банкингом называют технологии дистанционного банковского обслуживания, а также доступ к счетам и операциям, доступ к которым можно получить в любое время и с любого устройства, которое имеет выход в Интернет [7].

С внедрением новых технологий и упрощением проведения различных банковских операций на первый план стали выходить вопросы управления рисками. Так, одной из главных проблем сегодня является встраивание механизмов кибербезопасности в новые разработки финансово-кредитной сферы. Это становится острым вопросом, особенно в последнее время, поскольку только в 2017 г. число кибератак на компании и банки выросло в 2,3 раза, как сообщила первый зампред Банка России Ольга Скоробогатова на Гайдаровском форуме [1].

Сегодня существует огромное количество видов финансовой киберпреступности, которые по способам и методам противоправных действий охватывают огромный спектр инновационных технологий. Киберпреступность в кредитно-финансовой сфере начинала свое развитие с хищения персональных данных владельцев кредитных карт и использования их в преступных целях, а сегодня злоумышленники применяют «криминальное программирование» в целях получения доступа к цифровым активам банков [2].

В вопросе противодействия подобного рода криминальному поведению ведется значительная работа. Зампред Сбербанка Станислав Кузнецов на выступлении в Давосе на открытии Глобального центра кибербезопасности сказал, что киберугрозы сегодня становятся одним из основных факторов риска в таких сферах жизни, как экономическая, финансовая и социальная, что осознают все развитые страны, поэтому российский банк принимал активное участие в разработке данного Центра. Работа Центра представляла собой платформу государственно-частного партнерства, развитие которой будет происходить по трем ключевым направлениям: формирование сотрудничества между государственными и частными корпорациями на выгодных для всех условиях, создание всех условий для успешного обмена информацией и формирование исследовательского центра, который будет осуществлять объективную оценку и анализ текущей ситуации в области кибербезопасности на международной арене [3].

На наш взгляд, вопрос кибербезопасности в финансово-кредитной сфере, в первую очередь, затрагивает всех граждан, т. к. сегодня большая часть финансовых операций производится с помощью безналичного расчета и электронных операций, а также, несомненно, за-

ставляет государство в лице его правоохранительных органов реагировать на кибератаки, поскольку это ставит под угрозу кибербезопасность государства. На настоящем этапе подготовки правоохранительных органов недостаточно эффективного противодействия киберпреступности, поскольку, если в области финансово-кредитных отношений формирование соответствующих знаний производится на должном уровне, то в вопросах кибербезопасности злоумышленники находятся на гораздо более высоком уровне подготовки [4]. Отсюда следует сделать вывод, что необходимо повышение профессиональной подготовленности правоохранительных органов в вопросе противодействия киберперступности в финансово-экономической сфере для более эффективного решения этого вопроса.

Библиографический список

1. Число киберпреступлений в сфере новых финансовых технологий выросло в 2017 г. в 2,3 раза // TASS. – 2018. – 17 января.

2. Извлечение из доклада Центра Detica в партнерстве с Офисом информационной безопасности британской полиции и при поддержке Офиса Кабинета министров Великобритании [Электронный ресурс] / Электрон. дан. – Режим доступа: http://referatwork.ru/kiberprestupnost/ section-1.html, свободный. – Загл. с экрана.

3. Сбербанк объявил войну киберпреступности // Информационное агентство «365 дней». – 2018. – 27 января.

4. Марков Б. С., Иванов В. Ю. Руткиты: проблемы безопасности и тенденции развития // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 108–113.

5. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

6. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (том 2).

7. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – № 2 (том 2). – С. 30–38.

Д. Н. Захаров[1]

УГРОЗЫ СОВРЕМЕННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

К актуальным киберугрозам относятся: социальная инженерия; фишинг; специальные технические средства; вредоносное программное обеспечение; анонимность злоумышленников; нелегальные торговые площадки; криптовалюта; возможность перевода денежных средств через социальные сети и мессенджеры.

Социальная инженерия. Методы социальной инженерии направлены на получение информации, позволяющей однозначно идентифицировать пользователя. Например, его логин/пароль для доступа к определенным сервисам либо одноразового кода из СМС-сообщения, либо для выполнения определенных действий, которые может выполнить только авторизованный пользователь какой-либо системы.

Фишинг. Цель фишинга схожа с целями, в которых применяются методы социальной инженерии. Отличительной особенностью является использование веб-сайтов, приложений, которые либо полностью копируют оформление информационных сервисов, либо специально созданы для получения от пользователя необходимой злоумышленнику информации под любым предлогом.

Специальные технические средства. Использование специальных технических средств направлено на получение информации с банковских карт пользователя. Злоумышленников интересует PIN-код карты, а также информация с магнитной полосы банковской карты. Данный вид угрозы характеризуется высокой степенью риска, т. к. необходимо установить оборудование на клиентское устройство самообслуживания.

Вредоносное программное обеспечение. На текущем этапе развития информационных технологий использование вредоносного программного обеспечения особенно актуально. Способствует этому всеобщая компьютеризация. В современных мобильных устройствах применяется несколько разновидностей операционных систем. Все они характеризуются возможностью установки и запуска сторонних приложений. Рассматривая в качестве примера ОС Android. Приложения под данную ОС устанавливаются по умолчанию из магазина при-

[1] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Захаров Д. Н., 2018.

ложений Google Play Store, Samsung Store. В момент установки приложения у пользователя запрашиваются разрешения на работу с определенными функциями ОС, такими как отправка СМС, осуществление телефонных звонков. В последних версиях ОС данные разрешения запрашиваются у пользователя непосредственно в момент попытки вызова в приложении определенной функции. В случае использования альтернативных магазинов приложений требуется действие, которое ослабляет защиту устройства – разрешение установки приложений из неизвестных источников. Примером является использование магазина приложений Amazon Store, т. к. магазин представляет собой обычное приложение, которое необходимо установить. Зачастую после установки разрешение на установку из неизвестных источников не выключают. Регулярно появляются новости о том, что в магазине приложений Play Store обнаружено определенное количество зараженных вредоносным программным обеспечением приложений. Приложения для смартфонов также могут быть скачаны со сторонних сайтов и установлены. Обычно так поступают для того, чтобы использовать платные приложения бесплатно, например игры. Зараженное приложение может содержать в себе функционал для отправки СМС-сообщений. После запуска, приложение отправляет СМС на короткие номера, которые используются банками для взаимодействия с клиентами, например на номер 900 (ПАО «Сбербанк»), анализируя ответ, определяют, зарегистрирован ли номер телефона в мобильном банке, для выполнения команд от лица пользователя. Цифровыми следами в данном случае могут быть: номера счетов/телефоны, на которые осуществляется перевод денежных средств; источники загрузки зараженных приложений.

Анонимность злоумышленников. Существует определенный набор технологий, которые могут быть использованы для сокрытия информации о реальном IP-адресе. Примером подобных технологий являются TOR, I2P, прокси-серверы, VPN. Цифровыми следами работы пользователя в сети «Интернет» являются IP-адрес, а также записи в журналах событий веб-серверов или других сервисов. Основная цель, с которой используют подобные технологии, – это сокрытие реального IP-адреса злоумышленника. Реальный IP-адрес в сети «Интернет» не всегда позволяет однозначно идентифицировать компьютер, подключенный к сети «Интернет». Цепочка, по которой можно отследить пользователя в глобальной сети, выглядит следующим образом. IP-адрес и MAC-адрес устройства пользователя, устройство подключено

по Ethernet либо по Wi-FI к роутеру. На роутере остается информация о MAC-адресах клиентских устройств и о выданных этим MAC-адресам IP-адресах, а также о сроке аренды. Роутер подключен к сети провайдера. Со стороны провайдера нет информации о IP и MAC-адресе устройства клиента. У провайдера имеется информация о MAC-адресе и IP-адресе роутера, она содержится в журналах событий DHCP-сервера провайдера. На границе сети провайдера и глобальной сети «Интернет» установлено специальное оборудование, которое, как и роутер пользователя, преобразует IP-адреса. На этом оборудовании ведется журнал событий, который содержит информацию о IP и MAC-адресе роутера в сети провайдера, а также сроках аренды IP-адреса. Оборудование провайдера преобразует IP-адрес роутера в уникальный «белый» IP-адрес в глобальной сети «Интернет». Именно этот IP-адрес и остается в журналах событий веб-серверов. На этом этапе могут применяться различные технологии сокрытий IP-адреса.

Нелегальные торговые площадки. В свете последних событий, связанных с введением в строй реестра Роскомнадзора со списком запрещенных сайтов, у пользователей появляется желание обратится к сайтам из реестра запрещенных. Для того чтобы это осуществить, можно воспользоваться технологией TOR. В ресурсах, которые работают в сети TOR, имеются торговые площадки, на которых представлен ассортимент товаров и услуг, которые невозможно легально предлагать на рынке в Российской Федерации. Например, наркотические вещества, услуги по обмену валюты в любом варианте, предложения по работе, анонимный хостинг, анонимная электронная почта. Цифровыми следами работы пользователя на площадках в сети TOR и взаимодействия с другими пользователями для осуществления незаконного товарооборота являются PGP-ключи, которые невозможно запомнить и их необходимо записать в том или ином виде на носители информации; адреса Email, Jabber; номера мобильных телефон, баланс которых используется для приема денежных средств.

Криптовалюта. Понятие «криптовалюта» в законодательстве Российской Федерации на данный момент не определено. Также на данный момент отсутствует государственное регулирование эмиссии криптовалюты. Основываясь на законодательстве РФ, осуществлять эмиссию официальной валюты на территории Российской Федерации может только Центральный банк.

До сегодняшнего дня правовое регулирование криптовалюты не выработано.

Криптовалюта также обладает такими свойствами, как средство обмена и средство накопления.

Физическое лицо может использовать электронный кошелек по своему усмотрению. Юридическое лицо должно учитывать на балансе такой актив, но данный вопрос никак не регламентирован.

Как средство обмена. В договоре мены может учитываться только имущество. Криптовалюты не является имуществом. Они не имеют правового статуса Их возможно дарить, менять только имущественные права. Государство закрывает глаза, а в операциях физических лиц с криптовалютами мы не можем никаким образом защитить свои права на криптовалюты.

Хищение криптовалюты из кошелька не будет кражей, это будет признано в рамках ч. 2 ст. 14 УК РФ малозначительным деянием, не будет состава преступления, поскольку нет предмета. Под кражей понимается хищение чужого имущества, но криптовалюта не имущество.

В случае доказанности умысла на вывод похищенной криптовалюты в фиатную валюту такое действие можно квалифицироваться по правилам вегетационных знаков, как приготовление к краже на примере хищения другого имущества. Определение стоимости похищенного отсутствует в актуальных НПА.

Криптовалюта может существовать в Российской Федерации при определенных условиях. Она может оборачиваться внутри закрытой системы, когда есть соглашение между пользователями, которые подписывают некий договор.

Процесс эмиссии криптовалюты на компьютерном жаргоне называется «майнингом». Майнинг может быть направлен непосредственно на добычу криптовалюты либо на предоставление в аренду вычислительных мощностей. В любом случае в качестве вознаграждения будет получено некоторое количество криптовалюты.

Для того чтобы добыть криптовалюту, необходимо на компьютере запустить специальную программу, которая будет в процессе своего выполнения получать от определенного сервиса (пул для майнинга) вводные данные для расчета нового блока криптовалюты. Отсылая результаты своей работы на пул, после проверки будет получено определенное количество криптовалюты в качестве вознаграждения.

Криптовалюта является неким денежным суррогатом, который может быть использован для целей, схожих с обычными денежными средствами.

Операции с криптовалютой характеризуются некоторой степенью анонимности. Этому способствует базирование на технологии блокчейн (цепочка блоков), суть которой заключается в том, что большое количество компьютеров, являющихся частью этой цепочки, одновременно ведут журнал операций с криптовалютой (адреса отправителей и получателей), система открытых для пользователя ключей, а также адреса, где предыдущий и следующий блок в цепочке. Технология блокчейн характеризуется полной децентрализованностью. За счет большого количества подобных журналов подделка даже нескольких из них, например, за счет добавления в журнал новых транзакций, будет выявлена при следующей синхронизации журналов в цепочке. Именно по этой же причине каким-то образом заблокировать работу данной технологии в масштабах определенной страны невозможно.

Тем не менее технология блокчейн находит свое применение в банковской сфере, например, для быстрой отправки активов, построению доверительных систем обмена данными, где никто никому не доверяет.

В Росреестре при регистрации недвижимости. В Минздраве для рецептуры лекарств. Правовое положение блокчейн регулируется законами об информации…, о стандартизации…

Юридическая значимость записи в блокчейн. Она может быть использована как электронное доказательство.

Процесс движения криптовалюты характеризуется несколькими этапами – это эмиссия, покупка товаров/услуг, спекуляция на бирже, доходы за конвертацию криптовалюты и т. д.

Наиболее популярными криптовалютами являются Bitcoin, Etherium, Monero и другие.

Криптовалюты характеризуются условной степенью анонимности, идентифицировать владельца кошелька можно только по косвенным признакам. Например, номер кошелька записан в текстовом файле на носителе данных пользователя.

С точки зрения следствия операции с криптовалютой оставляют определенные цифровые следы. В качестве примера рассмотрим цепочку добычи криптовалюты, вывода из пула на кошелек или спекуляцию на бирже.

Для того чтобы начать добывать криптовалюту на определенном сервисе, необходимо зарегистрироваться на нем и получить пару логин/пароль и URL-адрес для обмена результатами майнинга. По прошествии некоторого времени будет добыто определенное количество

криптовалюты, которое необходимо вывести из пула. Для вывода доступны следующие варианты: на электронный кошелек либо на обменник, либо на счет биржи криптовалют.

В любом случае вывода каждая такая операция имеет определенный цифровой след – уникальный хеш транзакции.

В сети «Интернет» существуют сервисы для отслеживания транзакций любой криптовалюты, необходим только ее хеш. Результатом работы данного сервиса являются идентификаторы транзакций по добыче того блока криптовалюты, из которого был осуществлен перевод, а также номера кошельков на которые был осуществлен вывод.

Кошелек представляет собой программное обеспечение, которое может функционировать в качестве сервиса в сети интернет, либо программы на компьютере. Характерной особенностью является требование вести журнал операций с валютой. На синхронизацию журнала требуется некоторое время. Также подобный локальный кошелек занимает несколько десятков гигабайт. Именно поэтому выбор многих пользователей – электронные кошельки в виде сервиса в сети «Интернет». Каждый кошелек имеет свой уникальный идентификатор, в рамках выбранной криптовалюты. Для регистрации на сервисе необходима пара логин/пароль, дополнительно необходима либо привязка номера телефона (для получения одноразового кода), либо использование технологии двухфакторной аутентификации (например, Google Authenticator).

Рассматривая случай, когда необходимо купить криптовалюту, можно прибегнуть к услугам цифровых обменников в сети TOR. В общем случае технология выглядит следующим образом. Необходим номер кошелька, на который будет зачислено желаемое количество криптовалюты. Далее, в качестве оплаты предлагается перевести денежные средства (например, в рублях) на счет мобильного телефона в течение некоторого времени. Впоследствии указанное количество криптовалюты будет зачислено на указанный кошелек. В качестве цифровых следов имеются: номера кошельков отправителя и получателя, хеш транзакции, номер мобильного телефона. Примерами преступлений могут быть: получение взятки, легализация преступных доходов, вымогательство, мошенничество, финансовые пирамиды.

Перевод денежных средств через социальные сети и мессенджеры. Одной из современные функций, которые предлагают некоторые социальных сети и мессенджеры, является возможность перевода денежных средств с привязанных к учетной записи банковских карт. В

качестве примера рассмотрим, каким образом это реализовано в популярной социальной сети ВКонтакте.

Для того чтобы осуществить перевод, необходимо, чтобы отправитель и получатель имели страницы в данной социальной сети с привязанными к ним номерами мобильных телефонов. Получатель денежных средств видит только имя отправителя, сумму перевода и комментарий. Для осуществления перевода не нужно знать номер карты получателя, т. к. получатель перевода – учетная запись в социальной сети. Получатель самостоятельно выбирает, на какую карту получить средства. Сумма одного перевода ограничена 75 тыс. руб. Отправка каждого перевода подтверждается вводом CV-кода карты и одноразового кода из СМС с номера. Также принимаются не персонифицированные карты.

В **заключение** необходимо отметить, что требуется совершенствовать подготовку сотрудников органов внутренних дел, не только на этапе первичного получения высшего образования, но и активнее привлекать должностных лиц из профильных подразделений для краткосрочного повышения квалификации. Необходимость подобного подхода обусловлена в работах [1, 2, 3].

Библиографический список

1. Гончар В. В. Особенности подготовки следователей по расследованию преступлений, в сфере высоких технологий / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 64–69.

2. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

3. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – №2 (том 2).

А. А. Крылов[1]

МОНИТОРИНГ УГРОЗООБРАЗУЮЩИХ ФАКТОРОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Проведенные в ФГКУ «ВНИИ МВД России» исследования показали, что одной из доступных и эффективных форм информационного обеспечения профилактической работы на различных предприятиях является мониторинг состояния экономической безопасности. Дело в том, что проведенные в стране экономические реформы принципиально изменили структуру производственных отношений. Сегодня многократно увеличилось количество хозяйствующих субъектов и повысился уровень их экономической свободы. Это привело к тому, что многие традиционные методы оперативного обслуживания предприятий и организаций различных форм собственности уже не являются столь же эффективными, как это было прежде, в условиях административно-командной системы и господства государственной собственности. Например; возникают проблемы с получением оперативной информации традиционными административными методами. Поэтому подразделениям полиции сегодня необходимы новые оперативно-разыскные технологии, учитывающие современные нормативные требования, и новый формат экономических отношений и производительных сил [1].

Сегодня в подразделениях ЭБиПК работа должна строиться таким образом, чтобы аналитики этих подразделений при помощи специального инструментария и новых технологий могли бы оперативно «сканировать» открытую информацию, анализировать ее и предлагать оперативным сотрудникам конкретные рекомендации на предмет того, где и какие появляются угрозы, способные породить преступления, где в данный момент наиболее высока вероятность совершения правонарушений и куда следует направить усилия оперативных сотрудников.

Новизна проведенного исследования состоит в том, что разработан методический инструментарий для мониторинга угрозообразующих факторов, способствующих криминализации экономических отношений. Из теории экономической безопасности известно, что при определенных условиях практически любая хозяйственная операция может

---

[1] Главный научный сотрудник ФГКУ «ВНИИ МВД России» доктор экономических наук, профессор. © Крылов А. А., 2018.

породить угрозы криминального характера. Поэтому был составлен большой перечень угрозообразующих факторов и предложена система показателей и индикаторов, которые способны сигнализировать о том, что та или иная хозяйственная операция превращается в угрозообразующий фактор, который в свою очередь может спровоцировать реальную угрозу и даже преступление. Таким образом, можно определить; где, на каком участке предприятия необходимо активизировать оперативную работу, чтобы выявить возможные преступления?

В основе проведенной работы лежат достижения теории экономической безопасности, возможности современных информационных технологий, результаты исследований ОРД ОВД в некоторых отраслях экономики и основы информационно-аналитической работы. Из теории экономической безопасности взят ряд основополагающих положений, во-первых, такие категории теории экономической безопасности, как угрозы и угрозообразующие факторы, их показатели и индикаторы. Например, угрозообразующие факторы – обстоятельства или процессы (правового, экономического, технического, социального и иного характера), внешне выглядящие, как нормальная хозяйственная деятельность или обычное явление, которые способны при определенных обстоятельствах привести к появлению реальной криминальной угрозы и таким образом стать причиной или условием, способствующим различным правонарушениям. Классический пример, получение кредита – угрозообразующий фактор; невозврат кредита – угроза; злостное уклонение от погашения кредиторской задолженности, ст. 177 УК РФ – преступление.

Во-вторых, понятие «криминализация» хозяйствующих субъектов – процесс вытеснения легитимных экономических отношений в деятельности хозяйствующих субъектов их криминальными разновидностями.

В-третьих, ряд закономерностей, доказанных теорией экономической безопасности: взаимообусловленность угроз и правонарушений; взаимосвязь специфики управления предприятием и появления различных угроз, в том числе криминального характера; объективная зависимость потенциальных и реальных угроз экономической безопасности от различных социальных и экономических показателей; возможность трансформации любых экономических процессов в угрозообразующие факторы.

Из теории ОРД были взяты наработки по выявлению криминальных схем, используемых участниками ОПФ при совершении преступ-

лений экономической направленности. Из информационно-аналитической работы были использованы методики оценки оперативной обстановки на основе общедоступной социально-экономической информации. Наконец, из информационных технологий используются общедоступные поисковики и базы данных. В итоге был разработан инструментарий, позволяющий находить, сканировать и оценивать целевую информацию. Все это позволяет сопоставлять различные события, находить связи между объектами, приводить разрозненные оперативно-разыскные сведения в логически стройную и обоснованную систему зависимостей. Фактически речь идет о проведении в новом формате оперативно-разыскной идентификации, диагностики, оперативно-разыскного прогнозирования и аналитического поиска.

Наши методики представлены в виде специальных матриц и алгоритмов действий. Ниже представлен пример использования разработанной методики для мониторинга угрозообразующих факторов на промышленных предприятиях.

Первым шагом мониторинга является криминологический анализ оперативной обстановки среды, в которой работает хозяйствующий субъект. Рекомендации по проведению такого анализа были разработаны в ФГКУ «ВНИИ МВД России» и уже более 20 лет успешно применяются различными территориальными и отраслевыми подразделениями полиции [2]. Информационные источники для такого анализа можно получить на порталах территориальных администраций и отраслевых ведомств.

Вторым шагом мониторинга экономической безопасности является экономико-правовой анализ хозяйственной деятельности. Методика проведения такого анализа также разработана учеными института [3].

Третий шаг мониторинга состояния экономической безопасности – криминологический анализ оперативной обстановки непосредственно на предприятии. В этом случае одной из главных задач является определение угрозообразующих факторов и на этой основе выявление и нейтрализации угроз экономической безопасности и возможных преступлений.

Все многообразие угрозообразующих факторов, способных привести к различным правонарушениям, например на промышленных предприятиях, сгруппировано по пяти направлениям, которые связаны с различными аспектами работы предприятия: хозяйственные операции; управленческие решения; процессы, происходящих в производ-

ственной части объектов промышленности; финансовые операции; причины и условия, способствующие коррупционной деятельности.

Для каждого направления хозяйственной деятельности разработана специальная матрица. Структура матрицы построена таким образом, чтобы аналитик, переходя в строке от столбца к столбцу, мог оценить происходящие события с точки зрения правонарушений, которые возможно за ними скрываются. Если анализ происходящих событий показывает, что за данным событием могут скрываться какие-то правонарушения, то в дальнейшем для их выявления следует использовать специальные оперативно-разыскные меры [4].

Алгоритм мониторинга достаточно прост:

1. Определяется одно или несколько направлений работы предприятия (хозяйственные операции; управленческие решения; процессы, происходящие в производственной части объекта промышленности; финансово-хозяйственные операции; причины и условия, способствующие коррупционной деятельности), где по какой-либо информации могут иметь место правонарушения. Последующая работа осуществляется с соответствующей матрицей.
2. Определив направление мониторинга аналитик должен оценить данное предприятие по каждому угрозообразующему фактору соответствующей матрицы.
3. Если на предприятии имел место какой-либо факт из перечисленных в матрице, необходимо его оценить, двигаясь по строке, слева направо.

Работа аналитика по такому алгоритму позволяет определиться с направлением, по которому необходимо развернуть оперативно-разыскные мероприятия и сбор дополнительной информации, которую потом можно использовать в доказательственной базе выявленных правонарушений.

На сегодняшний день проработаны лишь принципиальные вопросы организации мониторинга экономической безопасности хозяйствующих субъектов и методические основы мониторинга. Подробно проработаны вопросы мониторинга угрозообразующих факторов на промышленных предприятиях и на объектах строительства. Теперь стоит задача – разработать методическое обеспечение для мониторинга экономической безопасности на предприятиях других отраслей экономики, которые в большей степени подвержены криминализации, например, для торговых предприятий, транспортных организаций, для организаций жилищно-коммунального хозяйства и т. п.

Библиографический список

1. Крылов А. А. Информационно-аналитическая работа в сфере обеспечения экономической безопасности // Вестник экономической безопасности. – 2016. – № 2. – С. 298.
2. Методы анализа влияния различных факторов социально-экономической ситуации на состояние оперативной обстановки: методическое пособие / под общ. ред. М. М. Бабаева. – М. : ВНИИ МВД России, 1999.
3. Васильев Э. А., Корнилов Г. А. Экономико-правовой анализ в борьбе с преступлениями в рыбной отрасли. – М. : ВНИИ МВД России 2007. – С. 34.
4. Береснев Д. С., Иванов В. Ю. Исследование процедуры приобщения лог-файлов к материалам уголовного дела // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 26–29.

Е. А.* Рудых**[1], ***А. В. Долбилов[2]

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Мы живем в XXI в., тогда, когда человечество совершает стремительный скачок в области информационных технологий, которые настолько «врезались» в нашу жизнь, делают ее проще и даже в некоторых ситуациях мы уже не представляем жизни без них. К примеру, оплачивая коммунальные услуги с помощью пластиковой карты, подключив мобильный банк, теперь даже не нужно выходить из дома, не говоря уже о том, что раньше образовывались целые очереди, чтобы оплатить ЖКХ.

Благодаря информационным банковским технологиям мы можем экономить свое время. Но, перечисляя плюсы ИБТ, нужно иметь в виду, что преступность пробирается и на этот уровень. Проблема, которая возникает с появлением банковских карт, может быть изложена в вопросах: как защитить свою информацию и данные, которые она несет в себе от мошенников? Какие действия с банковскими картами можно совершать, а каких стоит избегать, чтобы обезопасить себя?

---

[1] Курсант 230 учебного взвода факультета подготовки сотрудников для подразделений экономической безопасности и противодействия коррупции МосУ МВД России имени В.Я. Кикотя. © Рудых Е. А., 2018.

[2] Заместитель начальника кафедры экономической безопасности, финансов и экономического анализа МосУ МВД России имени В.Я. Кикотя кандидат экономических наук. © Долбилов А. В., 2018.

Существуют несколько видов мошенничества, связанных с банковскими картами, чтобы лучше понимать, как не поддаться в руки злоумышленников, рассмотрим некоторые из них.

Во-первых, это скимминг – данный метод берет свое название от того прибора, с помощью которого мошенничество с использованием банковских карт осуществляется. Человек, который покушается на чужие денежные средства, считывает информацию с магнитной ленты, которая расположена на обратной стороне карты. Существует два способа для того, чтобы скимминг был осуществлен.

В первом случае мошенник – это лицо торгового или же какого-либо развлекательного предприятия, где происходит расчет за услуги с карт, предназначенных для платежа. Доверие клиента, ловкость рук и субъект преступления незаметно считывает всю информацию с карты, применяя скиммер, причем времени будет затрачено незначительное количество, буквально несколько секунд. Никаких подозрений в том, что вас могли обхитрить. Когда информация получена, мошенник делает дубликат вашей карты для того, чтобы снять деньги со счета без участия хозяина карты. Для того, чтобы не стать жертвой таких деяний, нужно быть предельно внимательным, когда производится оплата за услуги, иначе преступник скопирует всю информацию и хранящиеся в ней данные с вашей карты. Вы останетесь без средств, поэтому сохраняйте бдительность.

Во втором случае мошенники могут использовать скиммер вот так: он используется в виде накладки на щель для картоприемника. Изготовление такой накладки настолько выполнено профессионально, буквально точь-в-точь, что клиент банка, используя свою карту в банкомате, даже без задней мысли вставить карту туда. Данные, записанные на магнитной ленте БК, считываются скиммером и в дальнейшем используются преступником для изготовления дубликата. Совместно со скиммером мошенники используют накладку на клавиатуру банкомата либо устанавливают скрытую видеокамеру для фиксации вводимого клиентом ПИН-кода.

Кражи денег с банковских счетов возможно избежать путем особой внимательности, бдительности, а также еще совет состоит в том, чтобы пользоваться только знакомыми моделями банкоматов и если вдруг при виде банкомата у вас какие-то элементы вызывают подозрения, то лучше сразу отказаться от такого пользования, поскольку вы рискуете быть обокраденными. Не забывайте, что ПИН-код банковской карты не должен знать никакой посторонний человек, даже со-

трудник банка. Подойдя к банкомату, вы вводите пароль, постарайтесь чтобы люди, которые стоят с вами, не смогли высмотреть его. Любая карта без ПИН-кода – это всего лишь пластиковый мусор.

Фишинг – другой вид мошенничества, при помощи которого мошенники могут вас обмануть. Информацию о банковской карте у вас могут попросить путем переписок в личных беседах, путем СМС, представившись сотрудниками банка, причем предлоги могут быть совершенно разнообразные, но цель одна – получить данные БК жертвы [1]. Узнав все данные карты и номер мобильного телефона обманувшего, преступники от его имени в одном из сервисных центров мобильной связи восстановят карту, сказав, что якобы она утеряна, и смогут снять все средства со счета. Одним из примеров фишинга также служит тот факт, что жертвы могут переходить на неофициальные сайты, и тем самым зарегистрировавшись на таких сайтах, сами добровольно передают информацию третьим лицам [3, 4, 5].

Кардинг (англ. carding) – это род мошенничества, при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, т. н. «трояны» и «черви»).

При желании весь кардинг можно условно поделить на два условных куска:

1) в реале (это когда создается реальная, осязаемая копия карты);

2) в Интернете (когда вся вся афера проворачивается в сети) [2].

К уголовной ответственности по ст. 159.3 УК РФ за совершение мошенничества с банковскими картами может быть привлечено вменяемое лицо, которому на момент совершения исполнилось 16 лет.

Исследование криминогенной ситуации в России показало, что доля преступлений с банковскими картами растет с каждым годом. Наиболее частыми жертвами данного вида преступлений становятся люди пенсионного возраста из-за своей доверчивости и плохого понимая работы банковской системы. Никому и никогда не сообщайте атрибуты вашей банковской карты и данные секретного кода, тогда будете в безопасности вы и ваши близкие.

Библиографический список

1. Иванов В. Ю. Использование особенностей операционной системы windows для поиска следов, связанных с загрузкой файлов в ходе компью-

терного инцидента // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 154–156.

2. Осторожно, МОШЕННИКИ! URL: http://your-cash.blogspot.ru/ 2011/ 03/blog-post_13.html (дата обращения: 28.01.2018).

3. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

4. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (т. 2).

5. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – № 2 (т. 2). – С. 30–38.

***Ю. С. Крылова*[1], *А. В. Долбилов*[2]**

ПРОБЛЕМЫ И РИСКИ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ

В данной статье рассмотрены проблемы и риски использования криптовалюты; приведены основные минусы работы с ней, указаны примеры, подтверждающие негативные факторы купли-продажи криптовалюты.

Криптовалюта или, как ее еще называют, «электронная наличность» – это виртуальная денежная единица, измеряемая в цифровых монетах (coin). Эти монеты состоят из пакетов данных, зашифрованной информации, защищенной от копирования и подделки [1], также криптовалютой называют особую разновидность электронного платежного средства.

Как любые другие операции, связанные с высокой прибылью, рынок криптовалют несет в себе определенные проблемы и риски. Риск – это спутник любого рейдера или инвестора, вне зависимости от рынков, с которыми он работает. От него невозможно избавиться, зато можно уменьшить, сведя до минимального.

Криптовалюта, являясь электронным средством платежа, по сути, программным кодом несет риск быть зараженной вредоносными программами – программами для скрытого майнинга.

---

[1] Курсант 228 учебного взвода факультета подготовки сотрудников для подразделений экономической безопасности и противодействия коррупции МосУ МВД России имени В.Я. Кикотя. © Крылова Ю. С., 2018.

[2] Заместитель начальника кафедры экономической безопасности, финансов и экономического анализа МосУ МВД России имени В.Я. Кикотя кандидат экономических наук. © Долбилов А. В., 2018.

Скрытый майнер (Stealth miner, майнер-бот, ботнет) – программа, которая в автоматическом режиме ведет майнинг незаметно для пользователя. То есть это стороннее программное обеспечение, которое устанавливается на компьютер, использует его ресурсы и перечисляет все заработанные средства на кошелек разработчика [2]. Работа Stealth miner' на первый взгляд очень схожа с вирусом. Он также маскируется под системный файл, также совершает какие-то операции и грузит систему.

Он просто использует ресурсы процессора, чтобы добывать криптовалюту в кошелек своего создателя. И большинство антивирусов не могут найти, а значит, и обезвредить эту программу.

В подтверждение наличия указанной проблемы необходимо указать, что в октябре 2017 г. криптомайнер coinhive поднялся на шестое место в списке самых распространенных вредоносных программных продуктов Global threat impact index [3].

Кибератаки – вторая по масштабности проблема и частое явление в мире развивающихся криптовалют. Кибератака – это попытка испортить или скомпрометировать функции компьютерной системы, в целях выведения компьютеров из строя или для похищения важных данных.

Рост числа ddos-атак и попыток взлома во время взлета курса криптовалют уже стали нормой, и тому есть две причины. Во-первых, хакеры, которые воруют биткоины и альткоины в момент подъема на рынке срывают гораздо больший куш. Во-вторых, временные перебои в работе сервисов, вызванные крупномасштабными ddos-атаками во время оживленной торговли, позволяют злоумышленникам управлять курсами валют либо для собственной выгоды, либо для создания паники на рынке.

Так, в ходе кибератаки 26 января 2018 г. было похищено криптовалюты nem на $400 млн, от кражи пострадали 260 тыс. пользователей [4].

В настоящее время в мире отсутствует нормативно-правовая база, устанавливающая эталонные правила, регулирующие куплю-продажи криптовалюты. Из этого следует, что нет и механизмов правовой защиты как инвесторов, так и лиц, эмитирующих токены. Сейчас в некоторых странах уже идут попытки включения криптоинвестирования в правовое поле и придание криптовалютам официального статуса.

В целом, если рассматривать правовой статус криптовалюты в России, можно сказать, что эти средства, скорее, имеют статус нематериальных активов. Запрета на использование криптовалют и биткоинов в

стране нет, но и свободно распоряжаться монетами нельзя. В частности, покупки за биткоины могут квалифицировать как террористическую или преступную деятельность, что способствует серьезному наказанию, в том числе уголовному.

Что касается профессиональных занятий биткоинами, то без наличия полноценного правового регулирования достаточно просто зарегистрироваться как субъект предпринимательской деятельности и оформить полученные от купли, продажи, а также майнинга биткоинов доходы. Вот только операции с биткоинами нельзя обозначать как финансовые, т. к. сомнительно, что власти признают биткоин полноценной валютой или признают его финансовым средством.

Банкротство и закрытие бирж криптовалют также вызывают проблемы в использовании криптовалюты.

Примерами таких краж являются ограбление Coincheck на сумму около 58 млрд иен (около $534 млн) в результате хакерской атаки. Это больше, чем потеряла в 2014 г. биржа Mt.Gox, у которой были украдены биткоины на сумму $500 млн Ограбление Coincheck сравнивают с хакерской атакой на японскую же криптовалютную биржу Mt.Gox в 2014 г., в результате которой она потеряла около $500 млн в биткоинах. В общей сложности было похищено 850 тыс. биткоинов, из них 750 тыс. принадлежали клиентам, еще 100 тыс. – самой бирже [5]. Южнокорейская криптовалютная биржа Youbit объявила о закрытии и начале процедуры банкротства после того, как во второй раз за последний год оказалась жертвой хакеров. Неизвестные злоумышленники похитили около 17 % активов площадки [6].

Отсутствие гарантий на возмещение убытков является риском, который несут участники рынка криптовалют. Платформа для хеджирования (хеджирование – открытие сделок на одном рынке для компенсации воздействия ценовых рисков равной, но противоположной позиции на другом рынке) рисков криптовалютных инвесторов не предоставляет и не намеревается предоставить, а также отказывается от предоставления каких-либо заверений, гарантий или обязательств в какой бы то ни было форме какому-либо юридическому или физическому лицу, включая любые заверения, гарантии или обязательства в отношении достоверности, точности и полноты любой информации [7].

Потенциальная возможность краха рынка виртуальных денег также несет риск использования криптовалют.

Так, прийти к общему мнению по поводу развития рынка криптовалют очень непросто ввиду отсутствия центрального управляющего

(руководителя). В настоящее время не существует какого-либо плана или дорожной карты, в соответствии с которыми криптовалюта могла бы развиваться дальше. Для получения новых биткоинов будет требоваться все больше времени, а также новые вычислительные мощности. Если представить, что майнеры потеряют интерес к криптовалюте, то ее неизбежно ждет крах. Сообщество майнеров все чаще сталкивается с определенными страхами и неопределенностью. Некоторые эксперты говорят о том, что если в среде майнеров назреет мнение о том, что виртуальные деньги могут стать нелегальными, их можно будет похитить или заразить каким-то вирусом, то это неизбежно приведет к сильнейшему падению курса. Как только страх овладеет майнерами, они начнут массово избавляться от виртуальных накоплений, что в свою очередь крайне негативно отразится на всем криптовалютном направлении [8].

Все это характеризует еще одну проблему рынка криптовалют – нестабильность.

Кроме того, использование криптовалюты усложняется ввиду наличия на рынке новых инвесторов, которые приходят на рынок криптовалют ico (первичную продажу токенов). Довольно часто пользователи не могут отличить ico серьезных блокчейн-проектов от тех, что созданы с целью обогатить своих основателей и исчезнуть.

Концептуально ico позволяет блокчейн-компаниям собирать средства в децентрализованной манере, без привлечения посредников. Условно, стартапы зависят от платформ для краудфандинга, например Kickstarter или Indiegogo, которые помогают собирать средства через поставщиков финансовых услуг в сети, таких как Paypal. Но привлечение двух отдельных посредников в процесс краудфандинга увеличивает комиссии и непредвиденные риски в отношении собранных средств. Проблема Ico состоит в том, что компании или блокчейн-проекты часто не могут продемонстрировать свой потенциал на основе эмпирических доказательств или рыночных данных. И Ico больше походит на азартную игру для инвесторов, которые делают ставки на будущую цену их токена [9, 11].

Ценность Ico или его токенов строится только на предположениях инвесторов и предоставленных «дорожных картах» проектов.

Многие пользователи лишились криптовалюты по причине потери доступа к своему аккаунту. Они просто доверили данные той бирже, на которой работали [10, 12, 13].

Ошибка при вводе кода всего на одну цифру или его отправка на неправильный адрес также приводят к потерям. Транзакцию отменить нельзя, поэтому отправленная сумма не может быть возвращена. Таким образом, ошибочная транзакция пользователя также является проблемой использования криптовалюты.

Для устранения вышеуказанных проблем необходимо постоянно помнить о безопасности, регулярно мониторить рынок и самостоятельно принимать решения о приобретении и продаже криптовалюты.

Библиографический список

1. Филиппов Е. А. Криптовалюта: от «А» до «Я»: [Электронный ресурс] : http://zefir.site/wp-content/uploads/2017/10/krypto-book.pdf.

2. Подробно о скрытом майнинге, его обнаружении и удалении: [Электронный ресурс] : // https://miningbitcoinguide.com/mining /sposoby/skrytyj-majner-najti-i-udalit.

3. Check Point отметил рост активности вредоносного ПО для майнинга криптовалюты, особенно отличились CoinHive и Seamless: [Электронный ресурс] : http://www.remoteshaman.com/news/check-point-otmetil-rost-aktivnosti-vredonosnogo-po-dlia-maininga-kriptovaliuty-osobenno-otlichilis-coin-hive-i-seamless.

4. Биржа Coincheck возместит клиентам потери криптовалюты от хакерской атаки: [Электронный ресурс] : https://www.kommersant. ru/doc/3533301.

5. Произошло крупнейшее в истории ограбление криптовалютной биржи: [Электронный ресурс] : http://safe.cnews.ru/news/top/2018-01-29_ krupnaya_kriptovalyutnaya_birzha_ograblena_na_500.

6. Криптобиржа Youbit объявила себя банкротом после второй за год хакерской атаки: [Электронный ресурс] : https://forklog. com/kriptobirzha-youbit-obyavila-sebya-bankrotom-posle-vtoroj-za-god-hakerskoj-ataki/

7. Техническое описание DeHedge: [Электронный ресурс] : https:// dehedge.com/documents/dehedge-whitepaper-ru.pdf.

8. Три причины будущего краха криптовалюты: [Электронный ресурс] : http://www.invest-rating.ru/financial-forecasts/?id=11921.

9. Проверка благонадежности ICO: как отличить серьезные проекты от мошеннических?: [Электронный ресурс] : https://ethclassic. ru/2017/04/28/ico-due-diligence-how-to-separate-legitimate-projects-from-scams/

10. Шесть ошибок новичков в работе с криптовалютой: [Электронный ресурс]: https:// www.mycryptocrypto.com/ 6-oshibok-novichkov-v-rabote-s-kriptovalyutoj.

11. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации : сбор-

ник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

12. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. 2017. № 2 (том 2).

13. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. 2017. Т. 2. № 2 (20). – С. 30-38.

Е. А. Русскевич[1]

НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ (Ст. 274[1] УК): ДОСТОИНСТВА И НЕДОСТАТКИ КРИМИНАЛИЗАЦИИ

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [1], которым гл. 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274[1]).

Специальная уголовно-правовая охрана информационно-коммуникационного комплекса, обеспечивающего нормальное функционирование особо важных для общества и государства объектов, не является изобретением российского законодателя и встречается во многих современных правовых режимах.

Стремительно развивающаяся архитектура виртуального пространства не только качественно улучшает нашу жизнь, но и генерирует новые риски и угрозы. В связи с этим информационные ресурсы стратегического значения, связанные с обеспечением общественной и государственной безопасности, должны быть действенно защищены, в том числе путем дифференциации уголовной ответственности за посягательства на их доступность и целостность.

Редакция ст. 274[1] УК РФ представляет собой объединение трех традиционных для отечественного законодательства форм преступного

---

[1] Старший преподаватель кафедры уголовного права МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Русскевич Е. А., 2018.

посягательства на безопасность компьютерных данных и систем: неправомерный доступ, создание и распространение вредоносного контента и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

По смыслу ст. 274[1] УК РФ все эти деяния должны быть направлены против объектов критической информационной инфраструктуры. Таким образом, анализируемая уголовно-правовая норма конкурирует и является специальной сразу к трем статьям: 272, 273 и 274 УК РФ. В некотором смысле конструирование ст. 274[1] УК РФ противоречит сложившейся юридической технике отечественного уголовного законодательства. Установление более строгой уголовной ответственности за посягательства на объекты критической информационной инфраструктуры предпочтительнее было бы реализовать путем выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст.ст. 272, 273 и 274 УК РФ.

Анализируемая уголовно-правовая норма имеет бланкетный характер и предполагает обращение к Федеральному закону от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1].

Предметом преступления, предусмотренного ч. 1, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Нельзя не отметить, что установление данного признака на практике может вызвать значительные затруднения. Функциональная направленность вредоносной программы, т. е. ее предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным.

Специфическим предметом преступлений, предусмотренных ч. 2 и 3 выступают объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической

промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

Объективная сторона преступления, предусмотренного ч. 1, предполагает совершение любого из трех альтернативных действий: создание, использование или распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры. Состав по конструкции является формальным. Если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты критической информационной инфраструктуры, содеянное образует единое преступление.

Объективная сторона преступления, предусмотренного ч. 2, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным и считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. Таким образом, следует сделать вывод, что сам по себе неправомерный доступ (так называемое «чистое хакерство», осуществляемое из профессионального интереса без намерения причинить вред) по смыслу ч. 2 ст. 274^1 УК РФ не является преступлением.

Вред как конструктивный признак диспозиции, предусмотренной ч. 2 ст. 274^1 УК РФ, не конкретизирован. Системное толкование отечественного уголовного законодательства позволяет сделать вывод, что таковым является уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры.

Следует отдельно указать, что диспозиция ч. 2 ст. 274^1 УК РФ содержит признаки, по сути, составного преступления, поскольку указывает, что под неправомерным доступом следует также понимать

доступ с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ. Таким образом, ч. 2 ст. 274[1] УК РФ охватывает и не требует квалифицировать по совокупности неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274[1] УК РФ) или иных вредоносных программ (ст. 273 УК РФ). При этом, если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности.

Объективная сторона преступления, предусмотренного ч. 3, заключается в нарушении: правил эксплуатации (средств хранения, обработки или передачи охраняемой компьютерной информации; информационных систем; информационно-телекоммуникационных сетей; автоматизированных систем управления; сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации); правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи [4]. Состав по конструкции является материальным и считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. В отличие от ст. 274 УК РФ, характеризующейся двумя уровнями взаимосвязанных общественно опасных последствий, ч. 3 ст. 274[1] УК РФ не предполагает установления признака крупного ущерба.

Учитывая специфику объектов посягательства, следует отметить, что совершение компьютерных атак на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической или химической промышленности может содержать признаки и других преступлений, предусмотренных ст.ст. 205, 281, 275, 276 УК РФ и др.

Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включенные в соот-

ветствующий реестр. При неправомерном доступе (ч. 2) умысел может быть как прямым, так и косвенным. Субъективная сторона преступления, предусмотренного ч. 3 ст. 274^1 УК РФ, характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа может совершаться как умышленно, так и по неосторожности. Следует поддержать точку зрения Н. Ш. Козаева, что неуказание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных (автор формулирует данный вывод применительно к ст. 274 УК РФ) является упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление, совершенным по неосторожности, только если это предусмотрено соответствующей статьей Особенной части УК РФ [2].

Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предполагает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. К сожалению, действующая редакция ст. 274^1 УК РФ никак не учитывает данное деление, что представляется существенным упущением с точки зрения теоретико-правовых основ дифференциации уголовной ответственности. Полагаем, что в этой части уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует корректировки.

Библиографический список

1. Российская газета. – 2017. – № 167. – 31 июля.

2. Козаев Н. Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монография. – М. : Юрлитинформ, 2015. – С. 172.

3. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации / Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

К. В. Давыдов[1]***, М. Б. Кавешников***[2]

ТЕРРОРИСТИЧЕСКАЯ УГРОЗА И БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ

В настоящее время одной из главных угроз миру и стабильности является терроризм. Государствам, поддерживавшим террористические организации, крайне выгодная дестабилизация обстановки на границах России или сопредельных с Российской Федерации стран. Террористы используют любые доступные им виды вооружения и военной техники.

Сегодня можно заметить все увеличивающийся интерес силовых структур, гражданских организаций к такому виду техники как беспилотная авиация. Это вызвано целым рядом преимуществ беспилотной авиации по сравнению с пилотируемой, а именно:

– практическое отсутствие или минимум авиационной специфики, что позволяет эксплуатировать БЛА в неавиационных формированиях;

– отсутствие необходимости в аэродромах, аттестованных посадочных площадках и сопутствующей инфраструктуре;

– относительная изменчивость структуры комплекса с БЛА в зависимости от решаемых задач, продолжительности проведения и непрерывности работ и ряда других факторов;

– существенная мобильность комплекса с БЛА;

– более широкий диапазон погодно-климатических условий применения;

– отсутствие необходимости наличия у операторов навыков пилотирования;

– достаточно широкий диапазон допустимых перегрузок для БЛА в связи с отсутствием на борту пилота;

– беспрепятственное применение в районах природных и техногенных катастроф, когда применение пилотируемой авиации опасно, невозможно или нецелесообразно;

– достаточно низкая оптическая, акустическая и радиолокационная заметность БЛА;

---

[1] Слушатель 518 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Константин В. Д., 2018.

[2] Доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Кавешников М. Б., 2018.

– высокая живучесть БЛА при обстреле из стрелкового оружия, обусловленная низкими вероятностями его обнаружения потенциальным противником и попадания;

– существенно более низкая стоимость разработки, производства и эксплуатации;

– незначительная стоимость подготовки обслуживающего персонала и ряд других.

История беспилотной воздушной техники в отличие от пилотируемой авиации насчитывает немногим более полутораста лет, когда в 1849 г. Венецианская республика восстала против австрийского господства. В это время австрийские войска впервые применили беспилотные воздушные шары, которые автоматически сбрасывали аэробомбы на Венецию.

Бурное развитие БЛА началось в середине прошлого века в первую очередь в интересах Вооруженных сил различных государств.

Все это привело к тому, что к системам с БЛА проявляют повышенный интерес не только государственные (в том числе силовые) и коммерческие структуры наряду с любителями-авиамоделистами, но и различного рода террористические (экстремистские) организации, что дает основание рассматривать беспилотные летательные аппараты, как потенциальный источник террористической угрозы.

Необходимо отметить, что технический уровень развития современных БЛА вполне позволяет их использование при проведении терактов. В то же время проведенные предварительные расчеты по критерию «эффективность-стоимость» показали, что применение БЛА в террористических актах в настоящее время экономически нецелесообразно. Кроме того, существуют достаточно сложные проблемы организационного характера, затрудняющие использование БЛА в террористических целях, о чем будет сказано ниже.

Моделирование процесса инициирования различных рецептур типа ТНТ, ТГА, ПВВ-40 и им подобных в замкнутом объеме с фрагментируемой оболочкой на разных высотах полета по критерию максимальная площадь ($S_{об.max}$) охвата поверхности при заданных уровне потока ($\lambda_{зад}$) фрагментов оболочки и энергии соприкосновения ($E_{уд.зад}$) фрагментов с исследуемой поверхностью продемонстрировала эффективность процесса в достаточно узком диапазоне высот полета.

Поскольку диапазон высот достаточно узок, то и вывод БЛА на объект атаки часто сопряжен со значительными трудностями даже при использовании спутниковых навигационных систем.

Учитывая вышесказанное, основными проблемами, которые могут свести на нет использование БЛА в терактах, можно отметить следующие:

– достаточно узкий диапазон высот эффективного применения;

– особенности макро- и микрорельефа местности, городской застройки (линии электропередач, деревья, мачты, здания и пр.), что существенно снижает эффективность проведения теракта и может привести к потере БЛА;

– необходимость во многих случаях поддержания одновременного визуального контакта с БЛА и объектом атаки;

– необходимость в большинстве случаев, ручного наведения БЛА на цель (либо на всем участке полета, либо на конечном участке траектории);

– существенные ограничения дальности и надежности радиоуправления БЛА и получения видеоинформации в реальном масштабе при уменьшении высоты полета, особенно в условиях городов и горно-холмистой местности, в том числе и при использовании систем GSM, CDMA и прочих;

– необходимость доработки системы управления БЛА для размещения дополнительного канала управления устройством инициирования;

– доработки конструкции БЛА для совмещения оптико-электронной и ударной целевой нагрузки на одном борту при ограниченных массогабаритных характеристик аппарата;

– поддержание визуального контакта с БЛА, с объектом, ограничение дальности радиоуправления БЛА приводят к значительному увеличению времени пребывания оператора на одном месте, что может привести к демаскировке террориста-оператора БЛА;

– необходимость прохождения специальной подготовки по управлению БЛА.

Таким образом, для успешного и эффективного применения БЛА необходимо использование как минимум одного (в большинстве случаев двух) широкополосных каналов связи «борт-земля», что при удалении от объекта на расстоянии уже более 1 км приводит к существенным трудностям. Для «безопасного» использования БЛА с программным управлением необходимо увеличивать массу БЛА, что приведет к однозначной расшифровке мероприятия.

Из основных причин применения БЛА, как альтернативных средств теракта, можно выделить три:

1. Возможность поражения больших по объемам территорий и объектов, а также людей и животных по сравнению с применением таких же средств поражения на земной поверхности.

2. Проведение ни столько физической, сколько психической атаки на население и правоохранительные органы.

3. Возможность доставки средств поражения в места, труднодоступные для наземных объектов (автотранспортные средства, террористы-смертники).

Несмотря на то, что при подготовке к теракту и его проведении может использоваться практически любой комплекс с БЛА (в зависимости от цели конкретного террористического акта), наиболее привлекательными вариантами для осуществления своих замыслов террористическими организациями будут те, что удовлетворяют всем нижеперечисленным требованиям**:**

1. Возможность без излишних помех со стороны правоохранительных органов покинуть позицию исполнительного старта после выхода БЛА на заданный маршрут полета (при полете аппарата до цели в автоматическом режиме по программе) или после зависания над целью, либо после его вывода на цель и дальнейшей ликвидации (самоликвидации).

2. Скрытность и простота подготовки и проведения террористического акта, включая минимизацию трудозатрат при запуске самого БЛА.

3. Низкий уровень (отсутствие) шума и низкая возможность (невозможность) распознавания БЛА при визуальном контакте на удалении, достаточном для принятия превентивных мер правоохранительными органами по его обезвреживанию.

4. Устойчивость БЛА в полете при различных параметрах ветровой нагрузки.

5. Максимальная эффективность применения.

6. Экономическая целесообразность применения комплекса с БЛА вообще в ходе конкретной террористической атаки, а также комплекса с БЛА конкретного типа и класса по сравнению с традиционными способами.

Основными путями получения БЛА террористическими организациями могут быть:

– самостоятельное изготовление авиамоделей из запчастей, закупаемых на специализированных рынках;

– похищение комплексов с БЛА у добросовестных эксплуатантов;

– закупка серийных комплексов с БЛА с последующей их доработкой для совершения теракта;

– размещение спецзаказа на разработку и создания комплекса с БЛА с необходимым для проведения теракта оборудованием у разработчиков стран, враждебно настроенных к России, а также у нелегальных отечественных разработчиков (при их наличии или появлении).

Моделирование показало, что взлетная масса летательного аппарата должна быть не менее 1,5 кг. В ряде случаев может вырасти до 10…15 кг, что еще больше затруднит применение. Существенное влияние оказывает и время полета БЛА.

Необходимо отметить, что в настоящее время ВЗК РФ обязует эксплуатантов регистрировать беспилотные воздушные суда с максимальной взлетной массой более 250 г (пп. 1, п. 1 ст. 33). В то же время не проработаны технические меры по выявлению несанкционированных полетов таких БЛА.

С одной стороны, казалось бы, такое ограничение является жестким. По предварительным оценкам для успешной атаки подходят БЛА указанной выше максимальной взлетной массы и тяжелее. Однако стоит учитывать возможность проведения предварительной разведки объекта при помощи миниатюрных БЛА, в том числе и с использованием аппарата, запускаемых с ладони.

Объектами террористической атаки может оказать достаточно обширный круг объектов, что логично следует из диспозиции ст. 281 УК РФ «Диверсия». Полный перечень возможных объектов приводить не имеет смысла.

Исходя из этого, в ближайшее время применение беспилотных летательных аппаратов для достижения своих целей террористическими организациями маловероятно. Однако потенциальная угроза существует. Уже сейчас необходимо проводить исследования по поиску путей противодействия БЛА, как источнику террористической угрозы.

В заключение необходимо отметить, что рассматриваемая угроза является актуальной. Она технически осуществима. На сегодняшний момент применение БЛА в терактах нецелесообразно с экономической и часто весьма сложно с организационной точки зрения по сравнению с традиционными способами проведения терактов и диверсий. Но, тем не менее наука и техника на месте не стоят, и то, что неэффективно сейчас, может стать эффективным в ближайшие годы.

Раздел 2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В УСЛОВИЯХ КИБЕРУГРОЗ

М. А. Репко[1]***, К. К. Борзунов***[2]

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ И ЕЕ РЕШЕНИЕ

Актуальность проблемы определяется тем обстоятельством, что на территориальном уровне в органах внутренних дел (ОВД) существуют или группы сотрудников, или даже один сотрудник, обеспечивающие защиту информации.

1. **Объекты и процессы критической информационной инфраструктуры в ОВД.** К объектам необходимо отнести, прежде всего, подразделения полиции территориальных органов МВД России: подразделения по оперативному управлению силами и средствами органов внутренних дел (в том числе дежурные части); подразделения уголовного розыска (в том числе оперативно-сыскные подразделения); оперативно-поисковые подразделения; подразделения специальных технических мероприятий; подразделения оперативно-разыскной информации; подразделения собственной безопасности; подразделения по противодействию экстремизму; подразделения экономической безопасности и противодействия коррупции; подразделения участковых уполномоченных полиции; подразделения по исполнению административного законодательства; подразделения по делам несовершеннолетних; подразделения дознания; подразделения по контролю за оборотом наркотиков [5].

В некоторых из перечисленных подразделений имеются автоматизированные информационно-поисковые системы, обеспечивающие формирование и использование ведомственных учетов и баз данных, которые можно рассматривать как объекты критической информационной инфраструктуры.

В подразделениях полиции территориальных органов МВД России к процессам критической информационной инфраструктуры отно-

---

[1] Слушатель 517 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Репко М. А., 2018.

[2] Доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук, старший научный сотрудник. © Борзунов К. К., 2018.

сятся: внутренний документооборот; формирование и использование информационных ресурсов подразделения; информационное взаимодействие сотрудников (совещания и обсуждения, устные приказы и указания, служебные разговоры и т. д.).

2. **Угрозы безопасности информации в ОВД.** В процессе документооборота в ОВД наиболее вероятны угрозы, связанные с утерей (утратой) документов сотрудниками. Также потенциально возможна утечка информации по вине сотрудников, имеющих доступ к документам. В процессе накопления, обработки, использования и передачи данных и сведений, составляющих информационные ресурсы ОВД, наиболее вероятными угрозами могут быть утечка информации, утрата целостности информационных ресурсов и нарушение условий конфиденциальности, причины которых – корыстные мотивы, мотивы мести, нарушения правил работы с компьютерными информационными системами и самими данными, относящимися к ним. В процессе информационного взаимодействия сотрудников ОВД в рамках служебной деятельности наиболее вероятными оказываются угрозы, связанные с утечкой информации и нарушением условий конфиденциальности, причины которых кроются в свойствах характера личности (словоохотливость и доверчивость).

Анализ выявленных угроз свидетельствует о явно имеющейся проблеме обеспечения безопасности информации в деятельности ОВД, связанной с так называемым «человеческим» фактором. В силу этих причин организация деятельности сотрудников по защите информации в ОВД должна учитывать выявленную специфику.

Также анализ возможных угроз безопасности информации в ОВД показывает, что основной заинтересованной стороной выступают представители преступной среды, осуществляя противодействие следствию, дознанию и разнообразным мероприятиям оперативно-разыскной деятельности органов внутренних дел. Особенно опасными представителями противоборствующей стороны оказываются организованные преступные группировки и преступные сообщества, имеющие существенные финансовые и материально-технические возможности.

Крайне опасными и с непредсказуемыми последствиями оказываются ситуации, когда утечка конфиденциальной информации происходит случайно, в частности буквально в коридорах при разговоре сотрудников (как бы «мимоходом») в присутствии посторонних лиц, находящихся в ОВД по различным причинам.

3. **Организация деятельности сотрудников по защите информации в ОВД.** Анализ структурного построения территориальных органов МВД России [5] показывает, следующие результаты.

В территориальных органах внутренних дел на районном уровне лишь отдельные сотрудники (инспекторы) могут осуществлять делопроизводство или мероприятия по защите информации при условии, что в их должностных регламентах (инструкциях) предусмотрены соответствующие права и обязанности. Организацию их деятельности по соблюдению режимов конфиденциальности и защите информации осуществляет непосредственно их прямой начальник. При этом необходимо иметь в виду, что начальник территориального органа внутренних дел любого уровня несет ответственность за возникновение инцидентов безопасности информации в возглавляемом подразделении.

Таким образом, на районном уровне территориальных органов внутренних дел не удается в полной мере реализовать принципы организационной защиты информации, в частности непрерывности и комплексности.

В территориальных органах внутренних дел на окружном уровне возможно создание центра (группы) информационных технологий, связи и защиты информации, а также отдела (отделения, группы) делопроизводства и режима.

Начальники данных структур, каждый по своей линии, организуют и планируют деятельность подчиненных, связанную и с организационными, и техническими, и иными мероприятиями по защите информации и обеспечения режима конфиденциальности. При этом начальники указанных структур должны координировать общие мероприятия.

На окружном уровне территориальных органов внутренних дел отмечается больше возможностей по защите информации и обеспечения режима конфиденциальности. Но следует учитывать и увеличенный состав подразделений окружного уровня по сравнению с районным.

В территориальных органах внутренних дел регионального уровня количественный состав еще более растет по сравнению с уровнем округа: создаются более многочисленные отделы (отделения, группы, направления) отдельно по линии делопроизводства и режима, а также по линии информационных технологий, связи и защиты информации. Соответственно вырастают возможности тылового (материально-технического) и финансового обеспечения.

Исторически так сложилось, что наиболее сильно развитыми в организационном плане являются подразделения делопроизводства и режима. Данные подразделения выполняют технологически отработанные процедуры создания и исполнения документов, их регистрации и передачи, отправки в сторонние организации и архивы, контроля целостности и хранения документов, а также контроля выполнения требований режимов конфиденциальности.

Подразделения информационных технологий, связи и защиты информации в организационном плане более динамичны, поскольку не угасла активность процессов компьютеризации и информатизации в органах внутренних дел. Сотрудники этих структур осуществляют мероприятия (и организационные, и технические, и иные) по эксплуатации различных средств связи, по вводу в эксплуатацию информационных систем, их администрированию, их подключению к ведомственным телекоммуникациям, их эксплуатации, по защите информации.

Деятельность сотрудников указанных подразделений организуется, планируется и контролируется соответственно их прямыми начальниками.

4. **Рекомендуемые мероприятия.** В целях профилактики утраты документов сотрудниками в ходе документооборота необходимо использовать организационные мероприятия, связанные с усилением контроля внутренних потоков документов, исполнения документов сотрудниками подразделения, хранения документов сотрудниками на рабочих местах. Данные мероприятия по усилению контроля осуществляются сотрудниками секретариата ОВД или лицом, исполняющим обязанности делопроизводителя, с одной стороны, с другой – прямые начальники в работе с подчиненными сотрудниками должны регулярно уделять внимание вопросам сохранности служебных документов и обеспечению их конфиденциальности.

Выявление угроз безопасности информации, определяющихся корыстными мотивами или мотивами мести, в большей мере должно осуществляться прямыми начальниками и службой собственной безопасности. В данной ситуации лишь случайным образом предупредить угрозы безопасности информации могут либо сотрудники по защите информации на этапах контроля исполнения правил работы с компьютерными информационными системами, либо делопроизводители, контролирующие документооборот.

Следует особо отметить, что нарушение правил работы в компьютерных информационных системах сотрудниками может быть связано

и с нежеланием их исполнять по причине собственной лени и непонимания опасности их нарушения, и с попытками ускорения выполнения задач, поставленных вышестоящим руководством, когда предельно ограничивается время исполнения указаний. В данной ситуации сотрудники по защите информации имеют возможность осуществлять профилактику этих нарушений путем регулярного проведения разъяснительных бесед с сотрудниками в подразделении и их руководителями, а также путем прямого контроля исполнения правил работы с данными и сведениями в компьютерных информационных системах.

Сотрудники по защите информации или администраторы компьютерных информационных систем должны практически в круглосуточном режиме обеспечивать доступность информации в компьютерных системах с учетом разграничения доступа для сотрудников территориального подразделения ОВД.

Во всех подразделениях территориальных органов внутренних дел практически постоянно сотрудники ведут беседы с подозреваемыми, осуществляют опросы свидетелей, совершают допросы обвиняемых, обсуждают между собой планы последующих предпринимаемых действий и т. д. И в этой ситуации совершенно очевидно, что сотрудники по защите информации должны осуществлять регулярно (по плану) как организационные, так и технические мероприятия контроля разнообразных помещений на предмет возможной утечки речевой и видовой информации.

Слабо контролируемыми оказываются ситуации, когда происходит утечка информации или нарушаются условия конфиденциальности в силу наличия уязвимостей, связанных с социальными отношениями между людьми. Именно в этой ситуации играют первостепенную роль личностные качества человека – словоохотливость и доверчивость. В определенный момент сотрудник, не осознавая опасности, может совершить ошибку при общении со своими коллегами по службе или с хорошо знакомым, но посторонним человеком, что приведет к возникновению инцидента безопасности информации.

В качестве особых отдельных случаев можно отметить взаимодействия сотрудников органов внутренних дел с представителями средств массовой информации и с теми, кто скрытно пытается найти подходы в целях дальнейшего шантажа или установления коррупционных связей.

Здесь важной оказывается целенаправленная работа отдела кадров: качественный профессиональный отбор кандидатов на должности в

органы внутренних дел, обучение и повышение квалификации действующих сотрудников, определенно подобранная мотивация службы и т. д. Для действующих сотрудников важной является также поддержка службы собственной безопасности в условиях попыток воздействий на них со стороны преступных структур. Более существенную роль играют отношение прямого начальника к подчиненному, создание благоприятных условий работы и даже прямая при необходимости поддержка в указанных выше ситуациях.

Библиографический список

1. Аверченков В. И. Организационная защита информации: учебное пособие для вузов. – Брянск : БГТУ, 2014.

2. Степанов Е. А. Управление персоналом: Персонал в системе защиты информации : учебное пособие. – М. : ФОРУМ, ИНФРА-М, 2015.

3. Ярочкин В. И. Информационная безопасность: учебное пособие для студентов непрофильных вузов. – М. : Международные отношения, 2014.

4. Доктрина информационной безопасности Российской Федерации. Утв.Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

5. Приказ МВД РФ от 30 апреля 2011 г. № 333 «О некоторых организационных вопросах и структурном построении территориальных органов МВД России» (в ред. приказов МВД России от 14.06.2011 г. № 637, от 27. 06.2011 г. № 728, от 08.07.2011 г. № 815, от 29.07.2011 г. № 888, от 24.11. 2011 г. № 1167, от 18.05.2012 г. № 524, от 31.05.2012 г. № 556, от 29.06. 2012 г. № 650, от 11.12.2012 г. № 1091, от 28.05.2013 г. № 293, от 11.06. 2013 г. № 429, от 21.08.2013 г. № 636, от 15.10.2013 г. № 842, от 02.12.2013 г. № 940, от 10.12.2013 г. № 961, от 06.03.2014 г. № 141, от 18.03.2014 г. № 160, от 19.05.2014 г. № 424, от 10.06.2014 г. № 487, от 21.08.2014 г. № 716, от 23.08.2014 г. № 725, от 23.08.2014 г. № 726, от 10.09.2014 г. № 772, от 31.12.2014 г. № 1161, от 29.01.2015 г. № 63, от 23.04.2015 г. № 475, от 31.07.2015 г. № 805, от 31.07.2015 г. № 810, от 27.08.2015 г. № 840, от 23.09.2015 г. № 925, от 20.10.2015 г. № 994, от 27.10.2015 г. № 1009, от 11.12.2015 г. № 1164, от 31.12.2015 г. № 1266, от 12.05.2016 г. № 235, от 12.05.2016 г. № 239, от 18.05.2016 г. № 260, от 14.07.2016 г. № 391, от 22.09.2016 г. № 562, от 18.10.2016 г. № 657, от 06.12.2016 г. № 795, от 06.03.2017 г. № 99, от 16.03.2017 г. № 130, от 15.06.2017 г. № 380, от 26.06.2017 г. № 415, от 13.07.2017 г. № 458, от 20.07.2017 г.).

А. Л. Суворов[1], *В. И. Лустин*[2]

ЭТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Сформировавшийся в последние годы феномен информационной безопасности является необходимым фактором поддержания, развития и защиты информационного общества.

Правоохранительные органы, являясь важным социальным институтом, включенным в процесс обеспечения информационной безопасности в Российской Федерации, используют комплексную систему методов противодействия информационным угрозам: организационно-административные, законодательно-правовые, программно-технические, физические и морально-этические.

Этические аспекты информационной безопасности в правоохранительной сфере являются малоразработанной областью науки и практики, несмотря на то, что вопросы информационной этики в целом сегодня становятся актуальными для разных сторон человеческой деятельности. Раскрывая этические основы информационной безопасности в правоохранительной сфере, уточним основное понятие.

К сожалению, даже Уголовный кодекс Российской Федерации не оперирует понятием «информационная безопасность». Преступления, совершенные в этой области, рассматриваются как преступления, связанные с нарушениями создания и использования компьютерной информации (Гл. 28. УК РФ) [1].

На основе изучения взглядов ряда российских ученых и практиков определим информационную безопасность как необходимое ценностное и действенное качество информационной сферы, направленное на защиту ее целостности и ее объектов при наличии неблагоприятных внутренних и внешних воздействий.

Основными структурными элементами информационной безопасности являются: защита и обеспечение безопасности информационных потоков; защита субъектов информационного взаимодействия; формирование безопасного состояния информационной среды.

Этические аспекты информационной безопасности, в том числе вопросы профессионализма и профессиональной этики всех категорий, ра-

---

[1] Курсант 129 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Суворов А. Л., 2018.

[2] Старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Лустин В. И., 2018.

ботающих в соответствующей сфере, становятся сегодня актуальными для ученых и практиков. Это связано с тем, что, заменяя во многих областях свою деятельность техникой, особенно в духовной сфере человек становится близок к нарушению норм права и неправомерно вторгается в чужую жизнь, нарушая нормы информационной этики.

Информационная этика как система состоит из компьютерной этики, киберэтики и этических кодексов специалистов, работающих в сфере информационного обеспечения.

Компьютерная этика рассматривает все вопросы и проблемы, связанные с обеспечением безопасности, целостности, доступности и конфиденциальности информации; проблемы защиты интеллектуальной собственности; этические аспекты компьютерной безопасности, связанные с физическими, программными атаками; профессиональную этику и ответственность специалистов.

Киберэтика касается киберпреступлений в сети «Интернет»; нравственно-этических принципов коммуникаций в Интернете; этических аспектов научной работы с использований Интернета; этико-социальных последствий внедрения новых информационных технологий в глобальную сеть; проблем интернет-зависимости и игромании; вопросов цифрового неравенства и цензуры информации; проблем реализации межкультурного диалога через социальные сети.

Завершают систему информационной этики проблемные вопросы профессиональной этики.

Основные проблемы современной информационной этики: этические аспекты информационной приватности; нравственные ориентиры свободы в информационном обществе и информационная безопасность; этика интеллектуальной собственности в информационном пространстве; этические основы равноправного доступа к информационным ресурсам; этическое поведение в сети и противодействие информационным угрозам, способным нанести ущерб человеку и обществу.

Интенсивное использование глобальных сетей, прозрачность границ интернет-пространства несут со своими потоками в жизнь человека информационные риски и угрозы, вызывая многочисленные деструктивные явления. Правоохранительные органы в своей деятельности в рамках существующего информационного общества призваны законно, этически обоснованно препятствовать информационным рискам и угрозам, которые наносят ущерб нашему государству и его гражданам.

По данным правоохранительных органов, виновными в нарушениях информационной защиты в большинстве расследованных случаев ока-

зываются сотрудники организаций, которые знают меры информационной защиты и систему работы в этой области тех или иных предприятий. Безопасность информации во многом зависит от профессионализма людей, которые с ней работают, от их личностных качеств, от того, как соблюдаются принципы конфиденциальности, и т. д.

Сегодня расширяются профессиональные сферы, на которые должны распространяться этические нормы. Это профессии в области информационных технологий, информационно-библиотечного обслуживания, научные исследования на базе информационных технологий, журналистика, предпринимательство, госуслуги, правоохранительная деятельность в сфере обеспечения информационной безопасности и др.

Можно сравнить кодексы этики, принятые в таких организациях, как ISACA (Ассоциация аудита и контроля информационных систем), ISC (Международный консорциум по сертификации в области безопасности информационных систем), RISSPA (Сообщество профессионалов в области информационной безопасности). Везде указаны базовые этические принципы: честность, независимость, объективность, профессионализм, конфиденциальность. Все существующие этические кодексы специалистов в области информационной безопасности опираются на общечеловеческие ценности. Они не регламентируют выполнение конкретных действий, совершаемых в той или иной ситуации, а создают основу для принятия индивидуальных нравственных решений.

Особую важность этические кодексы приобретают в тех областях профессиональной деятельности людей, в которых они имеют дело с конфиденциальной информацией. Поэтому создание этического кодекса для сотрудников, обеспечивающих информационную безопасность в правоохранительной сфере, требует совместных усилий, исследований и разработок ученых и практиков.

Современная Доктрина информационной безопасности Российской Федерации, утвержденная в 2016 г. [2], может стать опорным документом для разработки этического кодекса соответствующих служб и сотрудников в правоохранительной сфере. Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности.

Согласно данному документу информационная безопасность Российской Федерации – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз.

Выстраивая концепцию этического кодекса специалиста по информационной безопасности в правоохранительной сфере, необходимо руко-

водствоваться национальными интересами России в этой области, указанными в Доктрине, а также учитывать обновление современных информационных угроз. Наиболее значимыми из них для нашей страны, как указано в Доктрине, являются: наращивание извне информационно-технического воздействия на информационную инфраструктуру нашей страны в военных целях; оказание информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации; увеличение объема материалов, содержащих предвзятую оценку государственной политики России; наращивание информационного воздействия на население России в целях размывания традиционных российских духовно-нравственных ценностей; возрастание масштабов компьютерной преступности; нарушение прав неприкосновенности частной жизни при обработке персональных данных с использованием информационных технологий и др.

Отдельно необходимо выделить угрозы, которые охватывают такую категорию граждан России, как дети и подростки, испытывая на себе различные информационные угрозы, они являются наиболее уязвимой, незащищенной, неподготовленной в этом плане частью населения. В различных информационных коммуникациях дети и подростки сегодня могут ощутить на себе неблагоприятные информационные воздействия и получить «дозу» вредной информации, которая может стать для них своеобразным «наркотиком» и подсадить либо на настоящие наркотики, а также подвигнуть к различным видам жестокости и насилия, развить экстремистско-националистические настроения, вовлечь в террористические организации.

Именно стражи порядка и законности призваны защищать права и законные интересы граждан России в условиях информационного общества и информационного пространства. Соответственно возрастает роль нравственно-этических регулятивов, при помощи которых должна быть выстроена вся система информационной безопасности в правоохранительной деятельности.

Библиографический список

1. Уголовный кодекс Российской Федерации. – Новосибирск : Норматика, 2016.

2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. http://www.pravo.gov.ru.

И. Р. Косачева[1], *А. В. Пузарин*[2]

ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ СОВМЕСТНО С ИННОВАЦИОННЫМИ ТЕХНОЛОГИЯМИ ЭНЕРГОСНАБЖЕНИЯ

Известно, что научный прогресс не стоит на месте, а развивается во всех отраслях, в том числе и в электроэнергетике. По ГОСТу Р. 53905-2010: «Энергосбережение. Термины и определения» под электроснабжением понимают обеспечение потребителей энергией (электрической энергией). Старое оборудование, устаревшие линии передач – из всего этого складываются тарифы сбытовых компаний и оплачивается потребителем. Для решения вопроса о формировании тарифов предлагалось устанавливать счетчики газа, воды, электроэнергии и тепла. Это послужило бы надежным контролем над каждым потребителем. Решение этой проблемы можно найти в системе АСКУЭ. Стоит отметить, что в АСКУЭ существуют несколько способов передачи. Одним из наиболее перспективных, на мой взгляд, является передача данных на базе счетчиков «Меркурий» по PLC модемам. «Меркурий-PLC» – это комплекс технического оборудования и программного обеспечения, который обеспечивает автоматизированный учет потребления энергии по низковольтным сетям с напряжением 0,4 кВ. Данная технология очень часто встречается в многоэтажных домах, дачных и сельских поселках. Отличительной чертой данной системы является отсутствие кабеля интерфейса, что значительно позволяет упростить дальнейшую эксплуатацию. На сегодняшний день есть два варианта построения системы: первый вариант это PLC-1 и второй PLC-2. В PLC-1 оборудование в основном ориентировано на создание АСКУЭ бытовых потребителей, потому что главный критерий– стоимость учета точки. Средой передачи данных для информационного обмена между концентраторами и счетчиками электроэнергии у нас выступают электросети с фазным напряжением 230В, 50 Гц. Высокую помехоустойчивость обеспечивает OFDM-модуляция с помощью

---

[1] Слушатель 517 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Косачева И. Р., 2018.

[2] Начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Пузарин А. В., 2018.

формирования результирующего сигнала путем сложения нескольких широкополосных сигналов в диапазоне от 10 до 91 кГц [1].

Задачами данного исследования будут являться: рассмотрение принципа работы АСКУЭ на основе модемов PLC; анализ объектов информатизации, использующих технические средства защиты информации по техническим каналам утечки информации; определение пересечения частотных диапазонов; проведение правового регулирования ТСЗИ и АСКУЭ; предложение по совместной работе технических средств защиты информации с шумогенераторами.

Как уже было сказано ранее, АСКУЭ – автоматизированная система, которая включает в себя: программное обеспечение; техническое оборудование для сбора, хранения, обработки информации и представлении данных по потреблению определенных энергоресурсов, что, естественно, способствует ускорению работы. Стоит отметить, что такая система облегчает финансовые расчеты, она также полностью контролирует весь процесс энергопотребления.

Принцип работы нашей автоматизированной систем заключается в том, чтобы создать условия своевременного и качественного контроля ресурсов, т. е. тепла, газа, электроэнергии и др. Сама модель системы представляет собой многоуровневую структуру из верхних и нижних секторов. Каждый из них выполняет свою работу и отвечает за обеспечение системы. Верхний сектор представлен в виде набора технических средств, которые собирают и обрабатывают информацию. В этот набор входят: адаптер – это устройство для сбора и передачи данных; модем, а также серверная часть, которая хранит и предоставляет данные операторам системы.

Нижний сектор состоит из счетчиков, трансформаторов тока и напряжения, иными словами, устройств для измерения самих данных. Программное обеспечение любой автоматизированной системы является неотъемлемой частью. Это связано с тем, что оно позволяет считывать данные с точек учета и предоставлять их пользователям системы. Ярким примером является программная оболочка АСКУЭ пирамида на рис. 1.

Данная пирамида состоит из уровня ИИК (измерительно-информационный комплекс). Его основная задача состоит в измерении конкретных точек учета: измерительные трансформаторы тока и напряжения; электросчетчики; устройства контроля за технологическими процессами (расходомеры, вычислители).

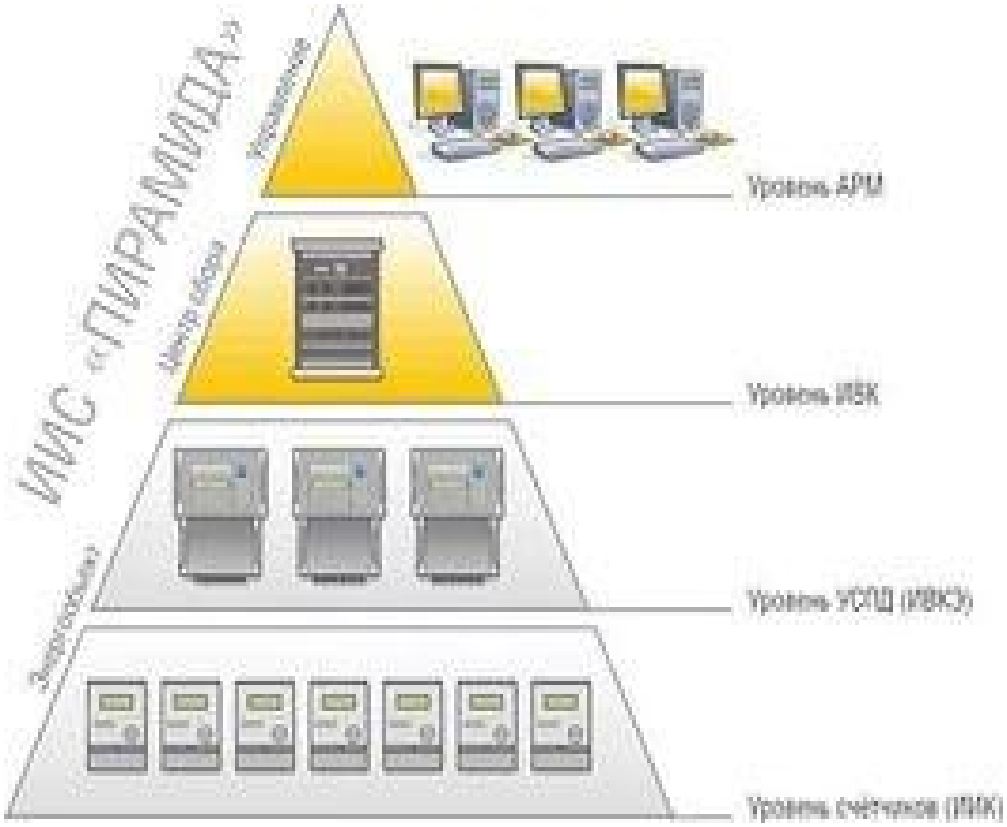


Рис. 1. Пирамида

Следующий уровень – накопление собранной информации ИВКЭ (информационно-вычислительный комплекс энергоустановки). Данный уровень включает в себя следующее: УСПД; контроллеры; каналообразующую аппаратуру.

И самый верхний уровень представляет собой информационно-вычислительный комплекс (ИВК). Здесь осуществляются автоматизированный сбор, обработка и хранение результатов измерения. ИВК включает в себя: серверное оборудование; техническое средство для построения локальной сети ЛВС.

На сегодняшний день возможны два варианта, как уже и говорилось ранее, формирования системы сбора данных. Они предлагают использовать такое оборудование как PLC-связи (PLC-I и PLC-II) (рис. 2), АСКУЭ на базе счетчиков «Меркурий» со встроенными модемами PLC (рис. 3).

Эта система отличается от ряда других тем, что контроль потребления осуществляется по сети 0,4 кВ с фазным напряжением 230 В, 50 Гц в отличие от АСКУЭ, которые построены на базе счетчиков с традиционным интерфейсом RS-485. За счет отсутствия данного интерфейсного кабеля снижается стоимость монтажных работ, что очень важно для каждого потребителя.

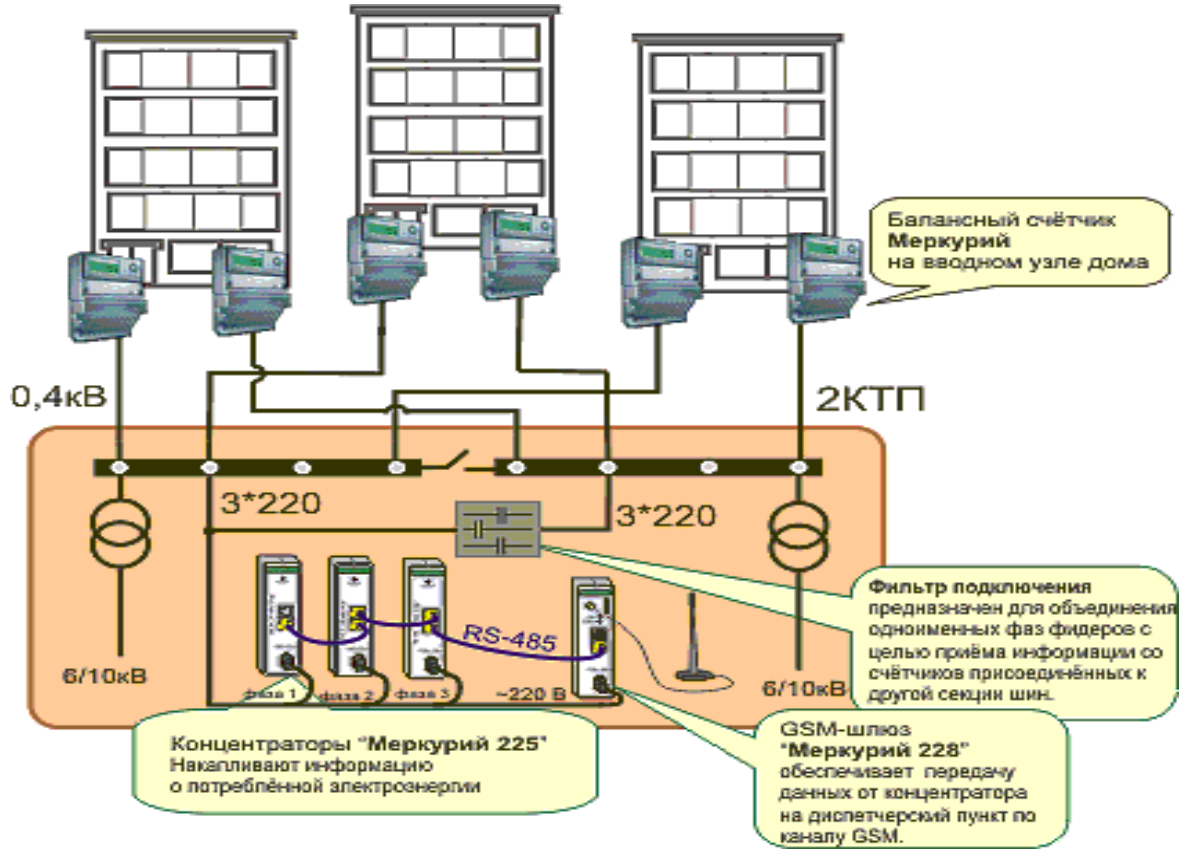


Рис. 2. Устройство АСКУЭ PLC

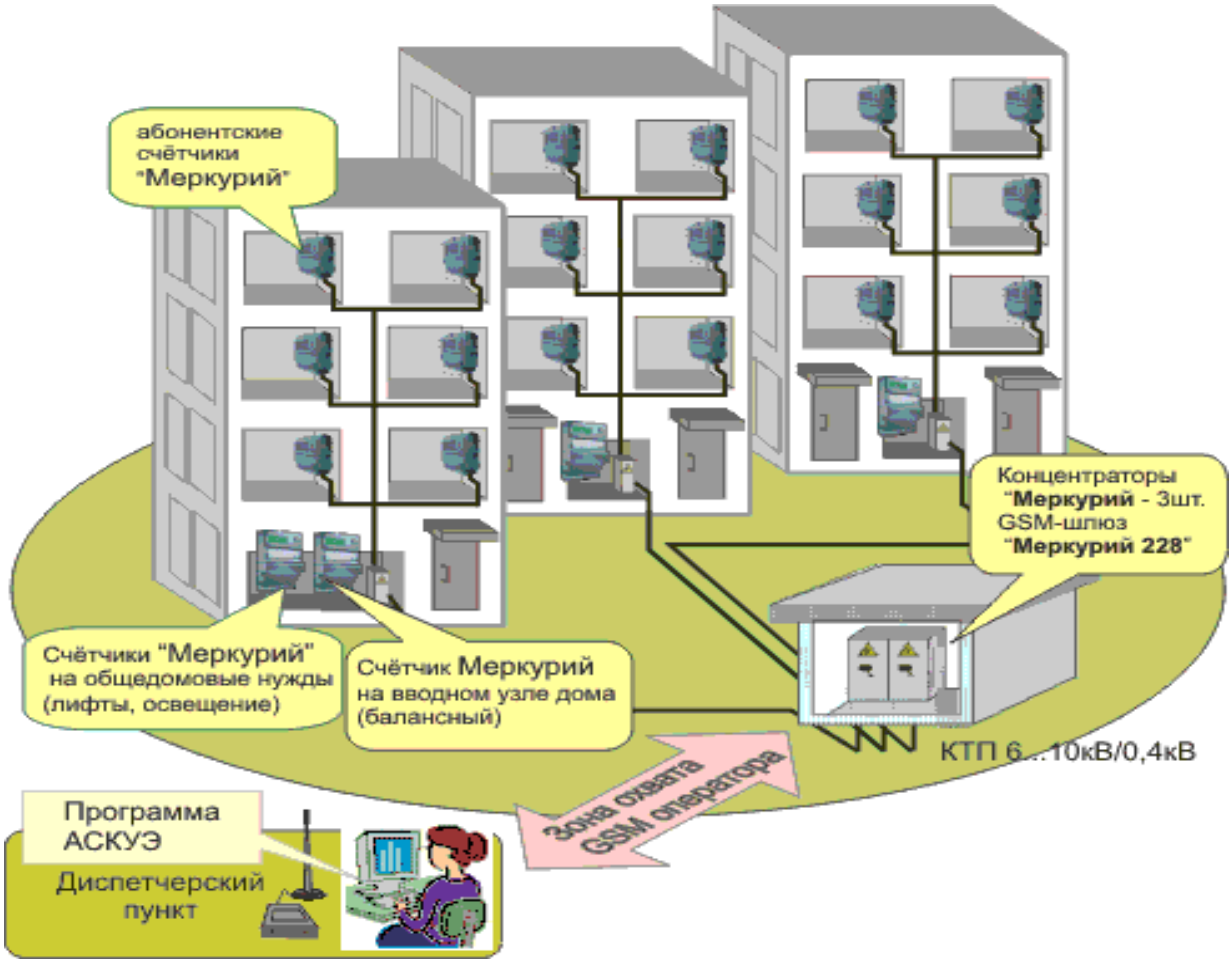


Рис. 3 Принцип работы АСКУЭ PLC

Высокая помехоустойчивость достигается при помощи использования OFDM-модуляции. Она формирует результирующий сигнал путем сложения нескольких широкополосных в диапазоне частот от 10 до 91 кГц. Концентраторы устанавливаются в любом подходящем месте четырехпроводной сети 0,4 кВ, к примеру, в электрощитовой жилого многоэтажного дома, но чаще всего на самой трансформаторной подстанции. Основные функции, которые они выполняют, – это обеспечение передачи данных счетчикам и прием информации о потребляемой энергии с ее последующим сохранением в собственной энергозависимой памяти. Кроме того, они осуществляют раздачу сигналов точного времени и изменяют режим работы счетчиков. Концентраторы оснащены интерфейсом RS-485, через который они посредством витой пары объединяются в единую локальную сеть друг с другом и различными дополнительными устройствами передачи информации (например, GSM-шлюз «Меркурий 228», радиомодемом и др. на удаленный компьютер диспетчерского пункта).

Для анализа совместного использования технических средств защиты информации и АСКУЭ проведем сравнение. В качестве примера будем использовать такие технические средства, как сетевой шумогенератор Соната-С1.

В нашем случае нас интересует такая техническая характеристика, как рабочий диапазон частот. Объединяя работу сетевого шумогенератора (Соната-С1) диапазон частот которого от 0,01 МГц до 3 МГц и АСКУЭ PLC-1, диапазон которого находится в рамках от 10 до 91 кГц (рис. 4), для защиты от несанкционированного доступа к информации – из наблюдения видится, что данный сетевой шумогенератор будет полностью блокировать наш полезный сигнал (рис. 5).

В настоящее время эпоха информатизации отражает внедрение все более новых высоких технологий в жизнедеятельность человека. Переходя к предметному рассмотрению технических каналов утечки информации, мы видим, как с каждым годом у стороны, противоборствующей с правоохранительными органами, расширяется спектр используемого ими арсенала методов и средств, отражающих всевозможные технические устройства. Используемые технические средства при столкновении противоборствующих сторон, а именно: специальных подразделений ОВД и их противников и субъектов, посягающих на информационную безопасность личности, общества и государства, отражен в широком спектре угроз и методов защиты; где одной из

наиболее опасных при рассмотрении угроз информационной безопасности является утечка информации по электрическому каналу.

Рис. 4. Соната-С1

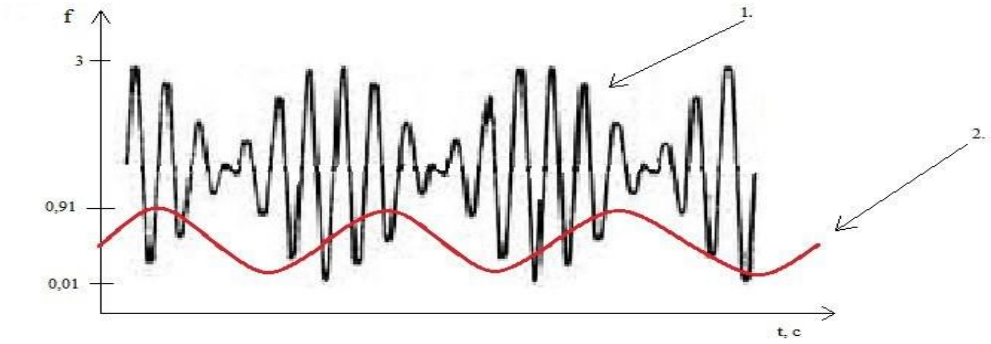


Рис. 5 Совместная работа АСКУЭ PLC-1 и Соната-С1

С целью повышения эффективности контроля и передачи энергоресурсов по электрическому каналу были взяты за основу принципы и функции АСКУЭ. В особенности был сделан акцент на некоторые технические параметры работы модемов PLC. Далее был взят шумогенератор, который в свою очередь применяется для блокирования утечки информации по электрическому каналу, был выявлен тот факт, что частотные диапазоны генератора перекрывают рабочий диапазон частот АСКУЭ. Таким образом, мы видим, что лицензированные технические устройства – шумогенераторы эффективны при использовании их в блокировании информации по электрическому каналу. С другой стороны, возможность использования ряда элементов типа модемов PLC и их принципов с целью более эффективного контроля потребления энергоснабжения на объекте информатизации на данном этапе проблематична. И для продуктивного решения данной проблематики необходимо расширить спектр технических устройств со схожим функционалом.

Библиографический список

1. Большунов А. Г., Пузарин А. В., Захаров Д. Н. Теоретические основы утечки информации и защита телефонных переговоров // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 30–34.

Н. С. Попов[1]***, А. В. Пузарин***[2]

ТЕХНОЛОГИЯ SOC (SECURITY OPERATIONS CENTER) В СИСТЕМЕ ОВД

SOC (Security Operations Center), Центр оперативного реагирования на инциденты информационной безопасности – организационная единица подразделения информационной безопасности, которая включает в себя людские единицы, процессы и технологии, предназначенные для получения ситуационной осведомленности в процессе обнаружения, локализации и предотвращения угроз информационной безопасности.

SoC включает в себя множество элементов, например, таких как Big Data, DLP-система.

Большие данные (англ. – big data) – разновидность подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного разнообразия для получения «читаемых» человеком результатов, наиболее эффективных в сочетании непрерывного прироста, распределения по многочисленным узлам вычислительной сети, которая может находиться как поблизости, так и задействовать через облачные технологии в пределах одного или нескольких государств, но «отработанную» информацию передавать на только один вычислительный центр.

Субъект big data необходим для: сбора и обработки больших данных: аналитики; инженерии больших данных; архитектуры больших данных и системной интеграции; разработки продуктов и услуг на основе больших данных; управления большими данными и системами на основе больших данных: проведения исследований в целях получения новых математических и технических решений для работы с большими данными.

Big Data кратко описывается с помощью четырех Vs: Volume (объем), Velocity (скорость), Variety (разнообразие), Veracity (достоверность).

Теперь о каждом поподробнее.

---

[1] Курсант 337 учебного взвода 3-И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Попов Н. С., 2018.

[2] Начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Пузарин А. В., 2018.

Объем. Реально большие объемы данных в физическом смысле. Тот объем данных, который раньше накапливался годами, теперь генерируется каждую минуту.

Новые инструменты больших данных используют распределенные системы, так что данные можно хранить и анализировать в нескольких географически распределенных базах данных.

Скорость. Сообщения в социальных сетях расходится по всему интернету в считанные секунды. Современные технологии позволяют анализировать данные на лету, даже не размещая их в базах данных.

Разнообразие. В недавнем прошлом рассматривались только структурированные данные, аккуратно встроенные в таблицы реляционных баз данных, например финансовые данные. Но фактически, 80 % мирового объема данных являются неструктурированными (текст, изображения, видео, голос и др.).

С технологиями больших данных теперь есть возможность проанализировать и свести воедино данные разных типов, такие как сообщения, разговоры в социальных сетях, фотографии, данные с датчиков, видео или голосовые записи.

Достоверность. Для значительного множества данных их качество и точность являются слабо контролируемыми (сообщения в Твиттере, сокращения и ошибки в разговорной речи, ненадежность и неточности контента). Новая технология позволяет теперь работать и с этим типом данных.

Теперь рассмотрим другой элемент, входящий в SoC.

Системы защиты от утечек конфиденциальной информации (Data Loss Prevention – DLP) предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через e-mail, социальные сети, чаты и т. д. Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности (защита информации от утечки).

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тен-

деров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т. д.

Основные функции DLP-систем:

– контроль передачи информации через Интернет с использованием E-Mail, HTTP, HTTPS, FTP, Skype, ICQ и других приложений и протоколов;

– контроль сохранения информации на внешние носители – CD, DVD, flash, мобильные телефоны и т. п.;

– защита информации от утечки путем контроля вывода данных на печать;

– блокирование попыток пересылки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий, использование карантинной папки;

– поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;

– предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.

Обычно система класса DLP включает следующие компоненты:

– центр управления и мониторинга;

– агенты на рабочих станциях пользователей;

– сетевой шлюз DLP, устанавливаемый на интернет-периметр.

Для чего нужно создание SoC:

– создание SoC находит уязвимые места и предотвращает атаки на них;

– SoC автоматизирует функции, которые и так уже сейчас есть в организации, что снизит расходы;

– часть подразделений готовы отдать свои функции в SoC и таким образом минимизировать свои расходы, вкладывая часть своих ресурсов в его построение.

Предоставление услуг SoC другим организациям окупит все вложения (так работают провайдеры сервисов по управлению безопасностью – Manager Security Services Providers – MSSP).

Примеры использования SoC: мониторинг распространения вредоносного кода, серверов Windows, Active Directory, утечек данных(DLP), устройств топ-менеджеров (VIP), IPS, привилегированных пользователей и контроль соответствия PCE отчетность и оповещения.

Преимущества SOC: ранняя идентификация и быстрое разрешение возникшей угрозы автоматизированной системы; устранение инцидентов до их выявления; минимизация финансовых потерь.

Предпосылкой для создания специализированного подразделения послужили следующие нормативные правовые акты:

1. Указ Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

2. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом Российской Федерации 03.02.2012 г. № 803).

3. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом Российской Федерации 12.12.2014 г. № К 1274).

4. Постановление Правительства Российской Федерации от 15.06.2016 г. № 541 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности».

5. «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 24.12.2016 г. № 149/2/7-200.

6. Проект Федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» Одобрены в первом чтении ГД РФ 27.01.2017 г.

7. Проект изменений в Уголовный и Уголовно-процессуальный кодексы Российской Федерации устанавливает ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Уголовный кодекс дополняется новой ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

8. Проект Федерального закона «О внесении изменений в ст. 16 ФЗ-149 «Об информации, информационных технологиях и о защите информации».

Деятельность центра мониторинга регламентируется:

Проект Федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» Одобрены в первом чтении ГД РФ 27.01.2017 г.

Проект изменений в Уголовный и Уголовно-процессуальный кодексы Российской Федерации, устанавливает ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Уголовный кодекс дополняется новой статьей 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру РФ».

Проект Федерального закона «О внесении изменений в ст. 16 ФЗ-149 «Об информации, информационных технологиях и о защите информации».

Типовой проект Соглашения по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Задачи, возлагаемые на главный центр ГосСОПКА:

– Реагирование на компьютерные инциденты.

– Координация действий субъектов ГосСОПКА.

– Обмен информацией о компьютерных инцидентах между субъектами ГосСОПКА.

– Обмен информацией о компьютерных инцидентах с иностранными государствами.

– Обмен информацией о компьютерных инцидентах с международными и неправительственными организациями.

– Анализ сведений, полученных в результате обмена данными с различными организациями и подведомственными учреждениями.

– Разработка решений и метод, по предоставленным данным.

При создании сегмента ГосСОПКА реализуются основные функции:

– инвентаризация информационных ресурсов;

– выявление уязвимостей информационных ресурсов;

– анализ угроз информационной безопасности;

– анализ данных о событиях безопасности;

– обеспечение процесса обнаружения компьютерных атак;

– регистрация инцидентов;

– реагирование на инциденты и ликвидация их последствий;

– установление причин инцидентов;

– анализ результатов устранения последствий инцидентов.

Предпосылкой создания SOC был Fusion Center. Отличительной чертой является то, что Fusion Center был предназначен для обмена информацией, а не круглосуточного мониторинга ИБ. Более того, первоначально, да и сейчас эти центры не имели ничего общего с кибербезопасностью. Они создавались под эгидой Министерства национальной безопасности или Минюста (а позже и на уровне отдельных госорганов или муниципалитетов) и позволяли обмениваться стратегической информацией между ФБС, Минобороны, МЧС, а также локальными администрациями и т. д. В первые годы Fusion Center, а их насчитывалось только несколько десятков, были достаточно бестолковы – они обменивались плохо структурированной информацией, которую сложно было анализировать, искать в ней взаимозависимости и строить на ее основе какие-то выводы и принимать решения. Например, в 2011 г. Fusion Center сообщил о взломе насосной станции системы водоснабжения в Подмосковье. Позже сотрудники ФБС опровергли данное заявление, доказав, что речь шла о легальном удаленном доступе администратора насосной станции.

Концепция «Фьюжн центра ИБ»:

– Создание и развитие экосистемы для обмена ИБ информацией и совместных действий как различных подразделений, так и различных компаний.

– Интеграция исторически различного функционала – ИБ, бизнес-подразделения, борьба с мошенничеством, соответствие положениям и стандартам и т. д.

– Координация аналитического функционала и совместных действий для предотвращения, обнаружения, управления и обучения на полученном опыте.

– Использование продвинутого функционала, такого как создание единого «озера данных» для информации, связанной с безопасностью.

– Использование на оперативном уровне технологий, идентифицирующих и детектирующих необычные паттерны поведения, которые могут являться указанием на незаконные действия в области кибербезопасности, мошенничества, кибератак, злоупотреблений, утечки и потери данных.

Прозрачность для руководства всей деятельности для своевременных управленческих решений.

Что же касается широкомасштабного применения SOC в Российской Федерации, то первым был Сбербанк России:

В Сбербанке по окончании второго этапа строительства центра безопасности ИТ-системы станут рассматривать миллионы подозрительных финансовых «событий» в день, для анализа которых будут внедрены средства искусственного интеллекта.

Центр безопасности 2.0. Сбербанк приступил ко второму этапу строительства центра информационной безопасности (Security Operational Center, SoC), который будет завершен до конца 2018 г. В ходе данных работ внедрено решение с использованием искусственного интеллекта, а также инструменты для работы с большими данными (bigdata) –рассказал зампредседателя правления Сбербанка Станислав Кузнецов.

В результате количество рассмотренных в день подозрительных «событий» в работе систем организации увеличилось до нескольких миллионов (сейчас этот показатель составляет 4 млн в сутки).

Первый этап по созданию SoC, который включал в себя внедрение SIEM-системы, ориентированной на сбор и корреляцию событий безопасности, был завершен в апреле 2016 г. Консультантом по реализации проекта выступила компания IBM, заключившая в декабре 2015 г. контракт со Сбербанком на 56,9 млн руб. Правда, по словам Кузнецова, в целом в проекте задействован ряд других компаний, названия которых он не сообщил.

В общей сложности работу центра безопасности обеспечивают более сотни сотрудников. Точное количество специалистов и местоположение SoC в Сбербанке не уточняют. Совокупный ИБ-бюджет банка в 2015 г. (включая строительство SoC) составил 1,5 млрд.

Б. И. Юдаков[1]***, А. В. Пузарин***[2]

ЦЕНТР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ (SECURITY OPERATIONS CENTER)

Сегодня вопросами построения Security Operation Center (SOC) интересуются практически все представители отечественной экономики: от страховых компаний и банков до крупных промышленных предприятий. Такой интерес вызван, прежде всего, постоянно совершенствующимися атаками и потребностью в современном инструменте противодействия им. Действительно, SOC является одним из ключевых компонентов подразделения информационной безопасности любой организации. В первую очередь он нацелен на мониторинг, детектирование и оперативную реакцию на инциденты и, как следствие, на сокращение ущерба и финансовых потерь, к которым тот или иной инцидент может привести [1].

При построении SOC важно помнить несколько моментов. Security Operation Center – это не только технические средства. Это команда, задача которой обнаруживать, анализировать, реагировать, уведомлять о возникновении и предотвращать инциденты информационной безопасности. Еще один немаловажный компонент SOC – это процессы, поскольку подразумевается взаимодействие между сотрудниками подразделения, отвечающего за мониторинг и реагирование на инциденты, а также между различными подразделениями (например, ИБ и ИТ). От того, насколько качественно выстроены эти процессы, будет зависеть эффективность работы SOC. Технические средства являются лишь инструментами, позволяющими автоматизировать часть процессов, которые функционируют в SOC. Ярким доказательством этому может послужить SOC одной из региональных энергетических компаний, в котором разбор инцидентов осуществляется сотрудниками подразделения без использования средств автоматизации. Но здесь нельзя забывать о том, что конкретно в этом примере поток событий от компонентов инфраструктуры невелик. Если же поток событий довольно большой, без SIEM-системы не обойтись, поскольку скорость реакции на инциденты будет низкой. Таким образом, формула идеального SOC выглядит так:

---

[1] Слушатель 517 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя.© Юдаков Б. И., 2018.

[2] Начальник кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Пузарин А. В., 2018.

SOC = Персонал + Процессы + Технические инструменты.

Более того, нельзя ни в коем случае забывать о том, что SOC не является коробочным решением. Это организм, все время эволюционирующий и адаптирующийся к постоянно меняющимся условиям окружающей среды. Для создания такого организма требуется взвешенный подход и множество усилий со стороны его владельца. Мы все прекрасно понимаем, что создание SOC – длительный процесс, который может затянуться на несколько лет. При этом внедрение только средств защиты может занять полгода. Мы все чаще слышим от своих заказчиков, что SOC у них еще не построен, но задача детектирования инцидентов и реакции на них стоит здесь и сейчас. И возникают вполне закономерные вопросы: с чего стоит начать, чтобы реализовать часть функций в короткие сроки, какие есть подводные камни и как их обойти, какие процессы стоит внедрить в первую очередь?

Хочется отметить, что зачастую при построении SOC первым делом покупается SIEM-система. Этот класс продуктов ИБ прочно ассоциируется с SOC, а зачастую между SIEM и SOC и вовсе ставится знак равенства. И уже только после этого приобретения создатели SOC в организации приступают к конкретной проработке целей и задач системы. Несмотря на туманные результаты такого подхода, он фактически является наиболее распространенным на практике. Мы бы рекомендовали чуть отложить радостный момент распаковки коробки с новенькой SIEM и начать именно с проработки ключевых параметров создаваемой системы: ее функций, архитектуры, задач. Сформулировать это необходимо письменно, что поможет архитектору SOC лучше разобраться в вопросе и донести «миссию» и ключевые параметры системы до коллег, руководства и подрядчиков. Хорошо, если данный программный документ получит под собой подпись высшего руководства компании. Итак, изначально лучше сосредоточиться на основных задачах SOC: проактивное предотвращение инцидентов ИБ, обнаружение и анализ нарушений ИБ в режиме реального времени, реагирование на инциденты, а также снабжение всех заинтересованных сторон в компании информацией о текущем уровне ИБ. Остальные задачи SOC можно считать вспомогательными.

К ключевым параметрам SOC можно отнести:

– организационную модель: интегрирован ли SOC в другое подразделение или является независимым, насколько он централизован, кому подчиняется, каких специалистов может привлекать для работы, и т. д.;

– выполняемые функции, исходящие из задач;

– уровень полномочий: полномочия SOC могут варьироваться от простых «советчиков» (оповещение, предоставление рекомендаций) до «спецназа» (в рамках реагирования на инцидент возможно конфигурирование оборудования, изменение бизнес-процессов, остановка систем и т. д.) [1].

Отдельно стоит рассматривать такие SOC, которые обслуживают внешние организации. Например, отраслевой, внутри группы компаний, предоставляющих услуги аутсорсинга и т. п.

Вопреки ожиданиям, основные подходы при построении таких SOC те же. Можно выделить более 40 основных функций, которые выполняют SOC: от сбора данных об инцидентах до взаимодействия с правоохранительными органами, от анализа вредоносного кода до повышения осведомленности сотрудников. Справедливости ради стоит отметить, что мы не встречали в своей практике SOC, успешно исполняющий все эти функции одновременно. Вероятно, таких систем и вовсе не существует. Как было отмечено выше, в начале строительства SOC справедливо правило «меньше, но лучше». Стоит сконцентрироваться на ключевых задачах, стоящих перед создаваемой системой, и описать процессы, обеспечивающие их выполнение. Нам необходимо как минимум собирать, хранить и обрабатывать данные от ИБ- и ИТ-систем, дать возможность пользователям сообщить о подозрительной активности, расследовать и реагировать на инциденты.

Команде SOC нужно иметь актуальную информацию об инфраструктуре, которую она защищает, и эффективно взаимодействовать с коллегами из других подразделений: ИТ- и ИБ-службы, HR, юристы, владельцы систем и пр. Без этого работу SOC представить сложно, поэтому именно с этого и стоит начать. Процессы и процедуры лучше фиксировать на бумаге. Во всех организациях принят разный уровень документирования, но хотя бы в минимальном виде на этом этапе оно должно быть, чтобы все участники процесса (а их немало) строили одно и то же. Только теперь, имея представление, что именно необходимо автоматизировать, можно переходить к выбору технических средств. Помимо традиционной SIEM-системы понадобится множество дополнительных инструментов, зачастую недорогих или бесплатных, но требующих от персонала SOC определенных знаний. Станут понятными и сами требования к «качеству и количеству» сотрудников.

Библиографический список

1. https://www.anti-malware.ru/analytics/Technology_Analysis/How_ fast_ run_SOC_Security_Operation_Center (дата обращения 07.02.2018).

С. Н. Золотарев[1], *Д. Н. Захаров*[2]

ЗАЩИТА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛАМ СВЯЗИ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время информационные технологии тесно переплелись с нашей повседневной жизнью, поэтому особую значимость и важность приобретают задачи защиты информации и информационных технологий. Безопасность в сфере информационных технологий – комплекс мер, и она должна быть построена как система. Все информационные ресурсы, подразумевая под этим сервер ОВД или компьютер пользователя, должны быть полностью защищены. Нельзя забывать и о защите файловых систем, сетей и т. п. Доступ к данным тоже должен быть безопасным, и люди, работающие с информацией, могут рассматриваться как звено в цепочке механизма, который обеспечивает работоспособность и безопасность всей системы.

Актуальность темы связана с увеличением количества преступлений в сфере информационных технологий, как следствие – с увеличением количества утечек информации. И использование ниже перечисленных методов защиты будет достаточным, если не для совсем исчезновения утечек, то до сведения их практически к нулю.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Канал связи – система технических средств и среда распространения сигналов для передачи сообщений (не только данных) от источника к получателю (и наоборот) [2] представлен на рис.

Рис. Канал связи

[1] Слушатель 517 учебного взвода 5-И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Золотарев С. Н., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Захаров Д. Н., 2018.

В различных источниках классификация каналов связи различается, но не сильно, приведем в пример одну из них ниже (табл. 1).

Таблица 1

Классификация каналов связи

Каналы связи					
Проводные каналы			Беспроводные каналы		
Витая пара	Коаксиальный кабель	Оптоволоконный кабель	Радиоканалы	Спутниковые каналы	Каналы в микроволновом диапазоне

Естественно, чтобы определить методы защиты информации, нам необходимо знать об угрозах, которые грозят информации. Для этого приведем их классификацию (табл. 2).

Таблица 2

Классификация угроз информации

Тип угрозы	Описание угрозы
Контроль доступа	Отсутствие регистрации конца сеанса при выходе с рабочей станции
	Отсутствие или некорректное построение политики контроля доступа
	Плохое управление паролями
	Неправильное использование программно-аппаратного обеспечения
	Неконтролируемая загрузка и использование программного обеспечения
	Пересылка паролей открытым текстом
	Отсутствие механизмов идентификации и аутентификации
	Неправильное разграничение доступа к общим ресурсам
	Отсутствие защиты мобильного компьютерного оборудования
	Отсутствие политик чистых столов и чистых экранов
Физическая безопасность	Незащищенное хранение
	Неадекватное или небрежное использование механизмов физического контроля доступа
	Отсутствие схемы периодической замены оборудования
	Недостаточное сопровождение средств хранения информации
	Отсутствие физической защиты здания
Управление коммуникациями и операциями	Неадекватное управление сетью
	Передача или повторное использование средств хранения информации без надлежащей очистки
	Отсутствие систем резервного копирования
	Неадекватный контроль изменений

Тип угрозы	Описание угрозы
	Отсутствие или несвоевременное обновление систем антивирусной защиты
	Отсутствие контроля за устанавливаемым ПО
	Нет четкого разделения обязанностей и ответственности
	Отсутствие доказательств отправки и получения сообщений
	Неконтролируемое копирование
	Нет разделения тестового и рабочего оборудования
Кадровая безопасность	Немотивированный персонал
	Нет регламента действий технических служб при увольнении сотрудников
	Безнадзорная работа внешнего персонала или персонала в нерабочее время
	Отсутствие механизмов мониторинга
	Неосведомленность пользователей в вопросах безопасности
	Отсутствие политик в области корректного использования технических средств
	Недостаточное обучение технического персонала в вопросах безопасности

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации [1].

Методы защиты информации, передаваемой по каналам связи, можно разделить на две группы: методы, основанные на ограничении физического доступа к линии и аппаратуре связи; методы, основанные на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

Ограничение физического доступа предполагает исключение (затруднение): непосредственного подключения аппаратуры злоумышленника к электрическим цепям аппаратуры абонентского терминала; использования для перехвата информации электромагнитных полей в

окружающем пространстве и наводок в отходящих цепях, сети питания и заземления; получения злоумышленником вспомогательной информации об используемом оборудовании и организации связи, облегчающей последующее несанкционированное вмешательство в канал связи.

Под вторым же методом защиты информации подразумевается использование технологии виртуальных частных сетей (VPN), позволяющей объединять территориально распределенные сети как с помощью защищенных выделенных каналов, так и виртуальных каналов, проходящих через глобальные общедоступные сети. Последовательный и системный подход к построению защищенных сетей предполагает не только защиту внешних каналов связи, но и эффективную защиту внутренних сетей путем выделения замкнутых внутренних контуров VPN. Таким образом, применение технологии VPN позволяет организовать безопасный доступ пользователей в Интернет, защитить серверные платформы и решить задачу сегментирования сети в соответствии с организационной структурой.

Также к этому методу можно отнести реализацию защиты информации посредством алгоритма асимметричных ключей и электронной подписи, защищающей информацию от подделки. Фактически данные, подлежащие межсегментной передаче, кодируются на выходе из одной сети, и декодируются на входе другой сети при этом алгоритм управления ключами обеспечивает их защищенное распределение между оконечными устройствами. Все манипуляции с данными прозрачны для работающих в сети приложений [3].

Подведя итоги, можно сказать, что обеспечить безопасность передачи информации по каналам связи между подразделениями ОВД довольно просто. Необходимо лишь придерживаться выше перечисленных методов; правовых, организационных и технических мер защиты информации.

Библиографический список

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Зюко А. Г., Кловский Д. Д., Коржик В. И., Назаров М. В. Теория электрической связи / под ред. Д. Д. Кловского: учебник для вузов. – М. : Радио и связь, 1999. – С. 15.

3. [Электронный ресурс] Защита информации в каналах связи и создание защищенных телекоммуникационных систем. URL: https://studfiles.net/preview/3183942/page:5/ (дата обращения: 13.12.2017).

***М. И. Титова*[1], *Е. Н. Клочкова*[2]**

ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ ИСОД МВД РОССИИ

ИСОД МВД России все плотнее входит в служебную деятельность сотрудников ОВД, становясь неотъемлемой частью работы различных подразделений. Система имеет четко построенную организацию для бесперебойной и быстрой работы в ней, большое количество общих и прикладных сервисов с возможностью разграничения доступа, а также грамотно построенную защиту – подсистему организации информационной безопасности (далее – подсистема ОИБ).

Подсистема ОИБ включает в себя:

1. Сервис управления доступом к информационным системам и ресурсам.
2. Подсистему антивирусной защиты.
3. Подсистему анализа защищенности.
4. Подсистему обнаружения вторжений.
5. Подсистему криптографической защиты информации.
6. Подсистему управления событиями информационной безопасности.
7. Дополнительные компоненты подсистемы ОИБ.
8. Организационную защита информации.

Конечно, данный этап развития ИСОД далеко не окончательный, и с каждым годом система совершенствуется, однако не обходится без недостатков, и заключается она в основном в организационной защите ИСОДа, именно эта проблема встает в рамках данной статьи.

Комплекс организационных мер является наиболее уязвимым компонентом, т. к. зависит от самого сотрудника ОВД. От своевременности обновления паролей для входа, от его бдительности и соблюдения мер и правил по обеспечению информационной безопасности при эксплуатации ИСОД МВД России. Данный аспект до сих пор до конца не изучен, и создание идеальной модели поведения сотрудника полиции при работе с техническими средствами, базами данных и другими инструментами, скорее всего, невозможно.

---

[1] Курсант 419 учебного взвода 4 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Титова М. И., 2018.

[2] Старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Клочкова Е. Н., 2018.

Решение задачи доступа сотрудников органов внутренних дел к информации с различных рабочих мест привело к тому, что значительно возросло количество точек доступа и количество самих пользователей, это ведет к неизбежному появлению человеческого фактора, особенно в условиях недостаточной грамотности в работе с компьютером и обеспечением информационной безопасности. Из-за недостаточного количества оформленных учетных записей логины и пароли, ключи ruToken передаются между сотрудниками, следовательно, невозможно реально отследить, кто пользовался системой. Также из-за требований безопасности по сложности паролей пользователям трудно их запомнить, при этом он еще и должен изменяться один раз в три месяца, следовательно, пользователи записывают их и, как правило, размещают в видимом месте, дабы не потерять пароль. Однако соблюдение минимальных требований мер безопасности, которые рассмотрены ниже, приведет к надежной защите информации.

Перед началом использования ИСОД пользователю необходимо вставить свой и только свой персональный идентификатор ruToken в любой USB порт компьютера или ноутбука и ввести пин-код. Идентификатор можно вставлять только в тот компьютер, где реализуется работа с ИСОД. Для того чтобы максимально снизить человеческий фактор, необходимо выполнять следующие правила:

– хранить свой логин и пароль в тайне, а именно: нельзя хранить его возле рабочего места, в ящиках, на мониторе, на столе и так далее, а идентификатор ruToken - в недоступном для других месте;

– не использовать посторонние носители информации;

– не открывать электронную почту, пришедшую от неизвестного отправителя;

– ни в коем случае не отключать средства защиты информации, установленные на рабочем месте.

Несоблюдение требований безопасности и информации может привести к хищению служебной информации либо нарушению целостности информационных систем ИСОД МВД России, а как следствие – к привлечению сотрудника в ответственности. Если обратиться к регламенту управления учетными записями сотрудников МВД России при доступе к сервисам…, то в нем прописано в 5 пункте ответственность пользователей, в котором говорится, что пользователь обязан, а не должен принимать все необходимые меры, которые помогут обеспечить безопасность идентификатора и пароля для доступа к учетной записи СУДИС, а также пользователь обязан обеспечить безопасность

ruToken, который привязан к учетной записи пользователя. Пользователь обязан незамедлительно обратиться к администратору доступа для блокировки учетной записи при компрометации (или подозрении на компрометацию) учетной записи сотрудника или при утере ruToken, что говорит о серьезности утраты ключа. Пользователь также несет персональную ответственность за инциденты, в результате которых были допущены несанкционированные изменения конфиденциальной информации сервисов ИСОД МВД России, внесенные с использованием его идентификатора (имени пользователя) либо с использованием ruToken.

Не стоит забывать и о том, что достаточно большое количество сотрудников ОВД обладают низкой грамотностью при работе с компьютером и другими техническими средствами ввиду того, что информационные технологии быстро развиваются. В этом ключе можно порекомендовать разработать программу обучения сотрудников основам средств вычислительной техники, программно-аппаратных и программных комплексов, в частности по работе с ИСОД МВД России. Проведение периодических семинаров и тренингов с последующей сдачей по пройденному материалу экзаменов или зачетов. Это поспособствует повышению компьютерной грамотности сотрудника, уверенному пользованию техническими средствами.

Для профилактики человеческого фактора можно порекомендовать проводить периодические инструктажи и контрольные занятия на знание основных организационных правил работы с ИСОДом.

Подводя итоги, следует сказать, что грамотно построенная подсистема обеспечения информационной безопасности, которую в свою очередь необходимо строго соблюдать, не дает полной гарантии защищенности. Иначе говоря, нельзя ограничиваться только программными и техническими мерами. Одним из ключевых аспектов обеспечения защищенности системы является организационная защита. Сотрудник органов внутренних дел может оказаться самым уязвимым звеном в обеспечении защиты информации в ИСОД МВД России. Надежность любых принимаемых технических мер обеспечения безопасности информации, в конце концов, зависит от человека. Из этого следует, что по степени реализации технических мер, основной акцент должен концентрироваться и усиливаться на неукоснительном соблюдении культуры обеспечения информационной безопасности на этапе эксплуатации ИСОД МВД России, сущностью которой является не только личная ответственность руководителя всех уровней за органи-

зацию защиты информационных ресурсов, а также строгое выполнение установленных правил обеспечения безопасности информации каждым отдельным сотрудником.

Библиографический список

1. Регламент управления учетными записями сотрудников МВД России при доступе к сервисам единой системы информационно-аналитического обеспечения деятельности МВД России [текст]: 2014.

***О. В. Симаков*[1], *В. В. Щерба*[2]**

МАТЕМАТИЧЕСКАЯ ОБФУСКАЦИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ПРОГРАММНОГО КОДА

Под обфускацией программного кода понимается любое ее изменение, при котором сохраняется вычисляемая программой функция, но в это же время программному коду придается такая форма, что извлечение из него важной информации о работе алгоритмов и структуре данных, содержащихся в этой программе, становится весьма трудоемким процессом. Главной целью обфускации (трансформации программного кода) является затруднение понимания программного кода третьими лицами, а также предотвратить [2].

Также можно сказать, что обфускацию можно расценивать как одну из разновидностей защиты программного кода. Но она значительно отличается от стандартных методов защиты, так как, прежде всего, она не предусматривает создания эффективных методов деобфускации, т. е. приведения программного кода к исходному виду, но при этом код после трансформации должен выполнять свои функции. Целью данной научной работы является первичное ознакомление с процессом обфускации, а также основными ее алгоритмами. При изучении обфускации со стороны математики необходимо понимать, что такое стойкость обфускации. Основные требования к стойкости в основном зависят от того программного обеспечения, к которым применяется обфускация.

---

[1] Симаков О. В.
[2] Старший преподаватель кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя.
© Щерба В. В. 2018

К сожалению, в настоящее время имеется значительное отличие теоретических задач обфускации от реальных задач, применяемых в жизни, т. к. на практике обфускация действенна лишь для очень узкого круга простых функций, например точечных. В то время как для более широких классов функций разработать функциональные методы обфускации практически не представляется возможным.

Таким образом, на данный момент невозможно точно сказать, что возможно создать единый и универсальный способ для трансформирования различных программных кодов единым обфускатором.

Процесс обфускации. Изучая данный процесс с точки зрения защиты программ, и трансформации кода без последующего возвращения данного кода к первоначальному виду (односторонняя обфускация), можно дать определение обфускации.

Пусть «TR» является процессом трансформации, тогда при «PR1 =TR=> PR2» программа «PR2» будет состоять из изменяемого программного кода «PR1». Такое изменение «TR» является обфускацией при соблюдении некоторых требований:

– программный код «PR2» по итогам трансформации будет сильно отличаться от программного кода «PR1», но одновременно с этим он сохранит свою работоспособность и будет выполнять такие же функции что и код программы «PR1», а также будет полностью работоспособным;

– изучение программного кода, а именно процесс реверсинженеринга, программного кода «PR2» будет весьма сложным, трудоемким и будет содержать в себе намного больше временных затрат, чем программного кода «PR1, либо вообще будет невозможным;

– при трансформации одного и того же программного кода «PR1» код на выходе обфускации «PR2» каждый раз будет различный;

– создание программы, возвращающей программный код «PR2» в его первоначальное состояние будет неэффективно.

Таким образом, получая разный код после процесса обфускации одной и той же программы, мы получаем уникальный программный продукт, и это преимущество можно использовать для оперативного поиска нарушителей (например, людей, которые, покупая продукт, занимаются продажей его копий). Для этого обладателем программного продукта создается контрольная сумма каждой копии программы, чей код прошел обфускацию, и затем она записывается в код программы совместно с информацией о лице, купившем программное обеспечение. Далее для выявления преступника необходимо будет определить

контрольную сумму копии и сопоставить ее с информацией, которая находится в базе, содержащей данные о каждом покупателе.

Из-за того, что код программы можно представить в двоичном виде или исходном виде какого-либо языка программирования, то процесс обфускации может быть произведен над любым видом программного кода, вследствие этого обычно выделяют два уровня процесса обфускации.

Низший уровень заключается в процессе трансформации кода над программным кодом, написанным на языке assembler или же непосредственно над двоичным файлом, содержащим машинный код.

Высший уровень подразумевает в себе осуществление трансформации над исходным кодом программы, которая написана на языке высокого уровня.

Трансформирование кода на низшем уровне имеет меньшее количество технологически связанных рабочих процессов и в это же время это является достаточно труднореализуемой задачей по ряду причин. Одна из них – это то, что должны учитываться особенности работы большинства алгоритмов работы, т. к. способ обфускации, подходящий для одной архитектуре, может не подходить к другой. Также процесс обфускации на низком уровне не получил большой популярности и в настоящее время малоисследован.

Далее рассмотрим основные существующие алгоритмы и методы обфускации, которые можно применить как для низшего, так и для высшего уровня.

Иногда довольно часто нецелесообразно изменять весь программный код, т. к. это может значительно снизить время исполнения программы, в этих случаях целесообразно осуществлять обфускацию только наиболее значимых частей кода.

Виды обфускации. Все процессы трансформации чаще всего делятся на виды, зависящие от того, каким способом изменится программный код.

Обфускация соединения. Самый важный этап реверс-инжиниринга основан на изучении структур данных. Это значит, что при обфускации кода необходимо усложнить представление структур данных, используемых программой.

Это достигается тем, что в процессе трансформирования кода представляемые структуры данных достаточно сильно усложняются. Для примера, при использовании данного метода происходит объединение независимых данных, или разъединению зависимых.

Далее представим основные методы, позволяющие произвести такое трансформирование: объединение переменных. Несколько переменных «v1,...,vk» могут быть скомпилированы в одну переменную «V», если их общий размер («v1,...,vk») не будет превышать размер переменной «V». Затем мы рассмотрим, более простой пример объединения двух коротких целочисленных переменных «X»,»Y» (размером 16 бит) в одну целочисленную переменную «Z» (размером 32 бита). Для этого мы будем пользоваться формулой:

Z(X,Y) = 2^16 * Y + X

Такая формула позволяет пренебрегать сложением и определять значение Y, т. е. пусть X = 12, Y = 4 => Z = 65536 * 4 + 12 = 262156, теперь, зная «Z» для поиска «Y», можно произвести следующую операцию 262156 / 65536 = 4.000183105 или приблизительно 4. При выполнении арифметических над значениями переменных «X», «Y» содержащихся в «Z» нужно держать во внимании вышеприведенную формулу, т.е.:

Z(X+n,Y)=2^16* Y +(X + n)= Z(X,Y)+ № ;

Z(X,Y-n)=2^16*(Y – n)+ X =2^16* Y -2^16* № + X =

= Z(X,Y)-2^16* № ;

и т. д. Исходный код до обфускации (язык Си):

```
short X =12, Y =4;
X +=5;
```

трансформируется в:

```
int Z =262156;
Z +=5;
```

Реструктурирование массивов заключается в запутывании структуры массивов [1]. Используя данный способ, мы разбиваем один из массивов на определенное количество более мелких подмассивов, в свою очередь они объединяются, и при этом размер конечного массива увеличивается. Например, один массив «@A» можно разбить на несколько подмассивов «@A1, @A2», при этом один массив «@A1» будет содержать четные позиции элементов, а второй «@A2» массив будет содержать в себе нечетные позиции элементов массива «@A». Поэтому такой фрагмент кода (PERL):

```
@A=qw{a b c d e f};
$i=3;
$A[$i]=...;
```

можно заменить на:

```
@A1=qw{240};
```

```
@A2=qw{135};
$i=3;
if(($i%2)==0){$A1[$i/2]=...;}
else{$A2[$i/2]=...;}
```

Если будем использовать сворачивание массива, то необходимо учесть, что это действие должно включать в себя создание двумерного массива из одномерного, другими словами, одномерный массив «A» из предыдущего примера, с размерностью 5 можно заменить на двумерный массив «B» с размерностью 2, после чего код (язык C++):

```
int A[]={1,2,3,4,5,6};
for(int i =0; i <8; i++)
{
A[i]= A[i]+1;
printf(«%d\n», A[i]);
}
```

Можно изменить на:

```
intA[2][3]={{1,2,3},
{4,5,6}};
for(int i =0; i <2; i++)
{
for(int ii =0; ii <4; ii++)
{
A[i][ii]= A[i][ii]+1;
printf(«%d\n», A[i][ii]);
}
}
```

Изменение иерархий наследования классов происходит из-за усложнения иерархии наследования с помощью создания дополнительных классов или ложного разделения классов.

Процесс деобфускации. Каждый раз, когда кто-то говорит о обфускации программного кода, многие задаются вопросом, а есть ли процесс, обратный обфускации, который мог бы помочь злоумышленнику вернуться к первоначальному коду программы. В настоящее время на данный вопрос достаточно трудно дать определенный ответ, но данный процесс все-таки существует и называется деобфускацией. Другим не менее значимым вопросом является проблема реализации данного процесса.

Многие считают, что процессом деобфускации можно считать оптимизацию программного кода, т. к. зачастую в процессе обфускации

в программном коде создается множество лишних операций, которые никак не влияют на работоспособность программы, и предназначены только лишь для усложнения процесса исследования кода злоумышленниками.

В связи с этим необходимо отметить тот факт, что большинство компиляторов в процессе компиляции конечного программного кода, автоматически производят оптимизацию, поэтому довольно часто компиляция кода прошедшего трансформирование, очень сильно снижает его защищенность. Но при использовании интерпретатора оптимизации не происходит, а значит, эффективность обфускации останется прежней.

Также к процессу деобфускации можно отнести процесс декомпиляции, с помощью которого при наличии двоичного кода программы мы можем получить наиболее точное представление данного, когда на языке высокого уровня, который является наиболее понятным для человека, из этого можно сделать вывод что это значительно упростит процесс реверс-инжиниринга программного кода продукта.

Несмотря на то что данный способ защиты программного продукта появился на свет сравнительно недавно, но уже сегодня существует немало данных, содержащих в себе информацию о попытках получения первоначального программного кода, а это значит, что в дальнейшем процесс деобфускации может значительно развиться.

На данный момент обфускация программного кода считается самой перспективной технологией, которая обеспечит программный код от вмешательства в него третьих лиц. Стремительно развивающиеся программные продукты и увеличение их стоимости заставляет производителей программного обеспечения искать наиболее совершенные методы защиты своих разработок и программных продуктов от несанкционированного использования третьими лицами.

Разработка наиболее совершенных методик трансформации программного кода, позволяющих обеспечить желаемого результата, является наиболее приоритетной задачей данных исследований.

Помимо функций защиты изменение программного кода с помощью оптимизирующих обфускаторов может увеличивать скорость выполнения программы.

Но помимо пользы неправильное использование обфускации также может нанести вред конечному программному продукту, т. к. обычно многие способы имеют множество побочных эффектов, таких как получение на выходе программы, непригодной к использованию, либо

при исполнении программы пользователь может получить новые ошибки.

Исследование и разработка алгоритмов, связанных с задачами в сфере информационной безопасности в наше время весьма актуальны, поэтому необходимо совершенствовать уже существующие виды обфускации, а так же создавать новые, для повышения уровни защищенности конечного программного продукта и исключения ошибок при его использовании.

Библиографический список

1. Вишневский А. В., Иванов В. Ю. Теневые операции с энергонезависимыми носителями информации (уязвимость bad-usb) // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2015. – С. 12–16.

2. Бегунков И. Д., Пузарин А. В., Захаров Д. Н. Программно-аппаратные средства защиты информации, передаваемой по техническим каналам связи // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 69–70.

Д. И. Якушев [1]

ПОСЛЕДСТВИЯ «ЛОЖНОЙ ТРЕВОГИ» В СИСТЕМАХ РАСПОЗНАВАНИЯ МВД

Проблемы технологического развития современного общества вообще и правоохранительной сферы, в частности, вызвали появление технологий автоматического распознавания образов. К этим технологиям можно отнести распознавание текста, государственных регистрационных номеров автотранспортных средств, отпечатков пальцев рук, устной речи, лиц и многие другие.

При решении задач распознавания образов производится сравнение двух образов: спорного и эталонного, в результате которого принимается решение об их соответствии. При этом рассматриваются ошибки первого и второго рода. Вероятность ошибки первого рода (равна 1 минус вероятность успешного распознавания) – это вероятность отвергнуть верную гипотезу. Вероятность ошибки второго рода («лож-

[1] Профессор кафедры Специальных информационных технологий Санкт-Петербургского университета МВД России доктор технических наук. © Якушев Д. И., 2018.

ной тревоги») – это вероятность принять неверную гипотезу. Величина этих вероятностей должна характеризовать качество системы. Однако, во-первых, некоторые производители эти характеристики системы не указывают, а во-вторых, по приведенным производителями характеристикам нельзя судить о работоспособности системы в конкретных условиях, поскольку условия получения обучающих образцов, использованных производителями при разработке системы, обычно отличны от предполагаемых условий эксплуатации. Поэтому единственным способом оценивания работоспособности системы в конкретных условиях является ее тестирование в этих условиях.

В настоящее время на вооружении МВД стоит аппаратно-программный комплекс «Поток», предназначенный, в числе прочего, для распознавания государственных регистрационных знаков движущихся транспортных средств и их автоматической проверки по базам розыска. Вероятность успешного распознавания номера > 0.9. Вероятность ложного распознавания не указана [1]. Были сообщения, что она составляет 0.0001, однако подтверждений этому найти не удалось. В случае констатации системой «Поток» факта нарушения правил дорожного движения автомобилем с распознанными номерами на адрес владельца автомобиля автоматически высылается штраф. В случае ложного распознавания номера штраф может быть оспорен в судебном порядке.

В системах распознавания государственных регистрационных знаков эталонные образы зафиксированы в ГОСТе [2], что может быть выполнено только для объектов искусственного происхождения, когда начертание символов и их взаимное расположение неизменно. Именно для этого случая разработана система автоматического распознавания «Поток». Под автоматическим имеется в виду принятие решения о соответствии сравниваемых образов без участия человека.

На вооружении МВД стоит автоматизированная дактилоскопическая информационная система «Папилон». Объектом распознавания в этой системе являются дактилоскопические отпечатки, которые, как и автомобильные номера, неизменны во времени, однако характеризуются случайным расположением папиллярных узоров. В настоящее время функционирует автоматизированная система, которая осуществляет поиск следов по существующей базе данных и предоставляет эксперту наиболее похожие результаты. То есть в этой системе решение принимает человек – эксперт. Вероятность успешного распознавания составляет > 0.85 [3]. Вероятность ошибки второго рода не

указана, видимо, в силу принятия решения экспертом. «Ложная тревога» при подобном подходе считается маловероятной и не рассматривается.

При распознавании устной речи и лиц какого-либо видимого постоянства можно только желать, что, естественно, сказывается на характеристиках систем распознавания. В распоряжении автора недостаточно информации для вынесения суждения о характеристиках систем распознавания речи. Устно заявляемая вероятность успешного распознавания, равная 0.999, представляется преувеличенной. При низкой вероятности «ложной тревоги» по положительным результатам распознавания устной речи может проводиться комплекс оперативно-разыскных мероприятий, результатом которого служит уточнение информации, полученной с помощью системы распознавания.

На качество распознавания лиц влияют характеристики, условия съемки и расположение камер наблюдения. Приведем требования к получению спорных изображений, разработанные компанией Видеомакс [4] (абл.).

Вероятность соблюдения перечисленных выше требований при съемке случайно попавшего в кадр человека в толпе, достаточно низка. Отсюда следует снижение заявленных характеристик систем распознавания лиц в реальных условиях.

При соблюдении требований и к эталонным, и к спорным изображениям заявляются следующие характеристики (система «Визирь», ЦРТ): 97 % успешно распознанных лиц на рубеже контроля при 1 % ложных срабатываний [5]. Заметим, что подразумевается получение исследуемых изображений на рубеже контроля, а не в толпе.

Таблица. Требования к получению спорных изображений

Характеристика	***Значение характеристики***
Расстояние между зрачками	≥ 60 пикс
Задний фон	Нейтральный
Освещение	Равномерное ≥ 150 лк
Отклонение плоскости лица от оси камеры	≤ 30^{o} как в горизонтальной, так и в вертикальной плоскости
Плотность пикселей	≥ 500 пикс/м во всей предполагаемой зоне распознавания
Фокусное расстояние и размер диафрагмы	Требуется подбор. Особенно актуально для длиннофокусных объективов

Характеристика	*Значение характеристики*
Время выдержки	≤ 0.01 с
Матрица камеры	≥ 5 Мпикс
Светосила объектива	≥ F1:1.4

Не рассматривая вероятность успешно распознанных лиц, обсудим вероятность ложных срабатываний системы на массовых мероприятиях. Допустим, что система выдает 1 % «ложной тревоги». Это означает, что при ста сравнениях в среднем происходит одно ложное срабатывание. Допустим, что на стадион пришло 50 000 зрителей, при этом имеется одно проверяемое лицо. На 50 000 сравнений 1 % «ложной тревоги» дает 500 человек, которые требуют реагирования правоохранительных органов. При увеличении количества проверяемых или при увеличении процента «ложной тревоги» увеличивается и количество подозреваемых. Проведение каких-либо оперативно-розыскных мероприятий в столь сжатые сроки при сотнях проверяемых лиц не представляется возможным.

По данным на 2015 г. система распознавания лиц, установленная в Мониторинговом центре Санкт-Петербурга, попросту была отключена по причине большого количества ложных срабатываний.

Да, безусловно, в число выявленных системой распознавания лиц входят и разыскиваемые преступники, о поимке которых с помощью подобных систем и сообщают средства массовой информации. Однако при этом необходимо отработать всех «ложно выявленных» системой распознавания лиц, что требует неприемлемо больших ресурсов и влечет за собой негативный общественный резонанс.

В этих условиях, не претендуя на общее решение вопроса, при проведении массовых мероприятий можно порекомендовать:

1. Тщательную разработку типовых действий сотрудников правоохранительных органов по реагированию на срабатывание системы распознавания лиц при проведении массовых мероприятий. Например, если каждый из зрителей должен иметь паспорт болельщика, то при проверке выявленного системой лица достаточно убедиться в отсутствии признаков подделки паспорта.

2. Помимо эталонной базы составлять базу изображений, полученных на рубеже контроля при прохождении на массовое мероприятие. Это позволит:

– Обеспечить максимально благоприятные условия получения изображений лиц, что понизит вероятность «ложной тревоги» и уменьшит количество проверяемых лиц.

– Проводить сопоставление данных системы распознавания лиц с данными документов и, возможно, биометрическими данными на рубеже контроля.

– Дальнейшие функции системы распознавания лиц будут состоять в сопоставлении лиц в толпе не с базой эталонов, а с базой лиц, прошедших рубеж контроля. В этом случае срабатывание системы будет заключаться не в совпадении, а в различии лиц, т. е. система будет поднимать тревогу в случае, когда лицо не проходило рубеж контроля.

В докладе не рассматривались системы 3D распознавания и системы распознавания на основе нейросетевых технологий, поскольку данных о работе таких систем в распоряжении автора недостаточно.

Библиографический список

1. Электронный ресурс: http://www.i-radar.ru/faq/36-apparatno-programmnyjj-kompleks -apk-potok.html (дата обращения 25.12.2017).

2. Государственный стандарт Российской Федерации ГОСТ Р 50577-93 «Знаки государственные регистрационные транспортных средств. Типы и основные размеры. Технические требования» // URL: http://base.garant.ru/12142212/#ixzz52acJMVmN (дата обращения: 25.12.2017).

3. Электронный ресурс: https://www.papillon.ru/rus/ 42?PHPSESSID=0b3096e372d809d1a6960297488f7a85#search (дата обращения: 28.12.2017).

4. Электронный ресурс: https://www.videomax-server.ru/support/ articles/raspoznavanie-lits-v-sistemakh-videonablyudeniya.

5. Электронный ресурс: https://www.speechpro.ru/product/sistemy-biometricheskogo-kontrolya-dostupa-ucheta-i-poiska/vizir (дата обращения: 29.12.2017).

Д. А. Камаева[1], А. В. Серезевский[2]

АНАЛИЗ СПОСОБОВ ОБХОДА ИЗВЕЩАТЕЛЕЙ В СОСТАВЕ СИСТЕМ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ, ПРИМЕНЯЕМЫХ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

Задача: Поиск решений по систематизации имеющихся знаний в области ОПС (охранно-пожарной сигнализации) и методах обхода данных устройств для упрощения работ по проектированию схем размещения систем ОПС применяемой для защиты объектов информатизации в ОВД.

Современные системы ОПС обычно являются совокупностью тех или иных совместно работающих ТС для получения, обработки и отправки информации на центральный пункт охраны, который обеспечивает контроль за поступлением информации о незаконных проникновениях, либо о попытках таких проникновений от объектов, которые охраняются.

Существует несколько видов общепринятых классификаций данных технических устройств: по способу приведения в действие; по условиям эксплуатации; по виду зоны контролируемой автоматическим извещателем; по физическим принципам; по способу электропитания; по сочетанию принципов обнаружения.

Существует список технических средств, в котором изложены основные виды извещателей. Их много, не говоря уже об их моделях. Каждый из них имеет свои особенности по физическим принципам, и именно эти особенности влияют на то, что устройства одного класса, но различных моделей имеют отличные друг от друга особенности при установке. К примеру, если говорить об оптико-электронных пассивных инфракрасных извещателях, сразу можно увидеть отличия в конструкции разных моделей, в особенности различных форм линзы Френеля. Различная форма этих линз меняет зону покрытия данных извещателей, а значит, некоторые из них можно установить на стену, а некоторые на потолок [4, 5, 6].

---

[1] Слушатель 517 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Камаева Д. А., 2018

[2] Старший преподаватель кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Серезевский А. В., 2018

Это первый факт, говорящий о требовании высокой квалификации специалистов, размещающих данные устройства на объектах информатизации, так как при их установке необходимо пресечь все возможные пути обхода извещателей, исключить попытки их саботажа, в общем говоря, обеспечить максимальную защищенность периметра объекта.

Второй факт – это множество способов саботажа (процесса нейтрализации работы датчиков) извещателей, что вынуждает проектировщика систем безопасности к размещению устройств таким образом, чтобы они взаимно прикрывали друг друга, чтобы исключить возможность их обхода. Самым простым и грубым примером такого размещения это если установлен извещатель «Штора», но к нему можно подобраться аккуратно, вырезав кусок стекла из окна. Для исключения таких возможностей можно установить вибродатчики на стекло либо звуковые датчики «Стекло».

Также всегда учитывается множество иных особенностей охраняемых объектов, даже материалы их конструкции или расположения внутри мебели.

Все вышеописанные детали свидетельствуют о том, что при обеспечении защиты необходимого объекта затрачивается большое количество времени для полноценного учета всех особенностей и уязвимостей как помещений, так и средств обнаружения незаконного проникновения с учетом взаимокомпенсации всех недостатков систем извещателей. Необходимо решение, которое позволило бы облегчить данную работу начинающим специалистам, тем самым сократить затраченное время на создание проекта систем безопасности на том или ином объекте. Существует множество классификаций тех или иных средств защиты объектов, но не существует классификации реальных способов их саботажа, а также путей решения этих проблем самыми выгодными и действующими методами. Возможным путем решения поднятой проблемы является создание такой классификации. Она несомненно, придаст наглядность любому процессу проектирования систем ОПС ОВД, тем самым значительно упростив данную работу, так как при использовании классификации саботажа и противодействия начинающему инженеру не придется тратить много времени на разборки справочной литературы, чтобы понять те ошибки, которые можно допустить при составлении проекта размещения извещателей на том или ином объекте.

Создавая такую классификацию необходимо придерживаться строгой системы трех блоков информации, представленной на рис.

Проведя анализ извещателей в системе охранно-пожарной сигнализации и методов их обхода, было найдено решение по систематизации имеющихся знаний для наглядности и упрощения плановых проектировочных работ по защите помещений и объектов в системе ОВД, а именно: создание классификации «Саботаж-Защита».

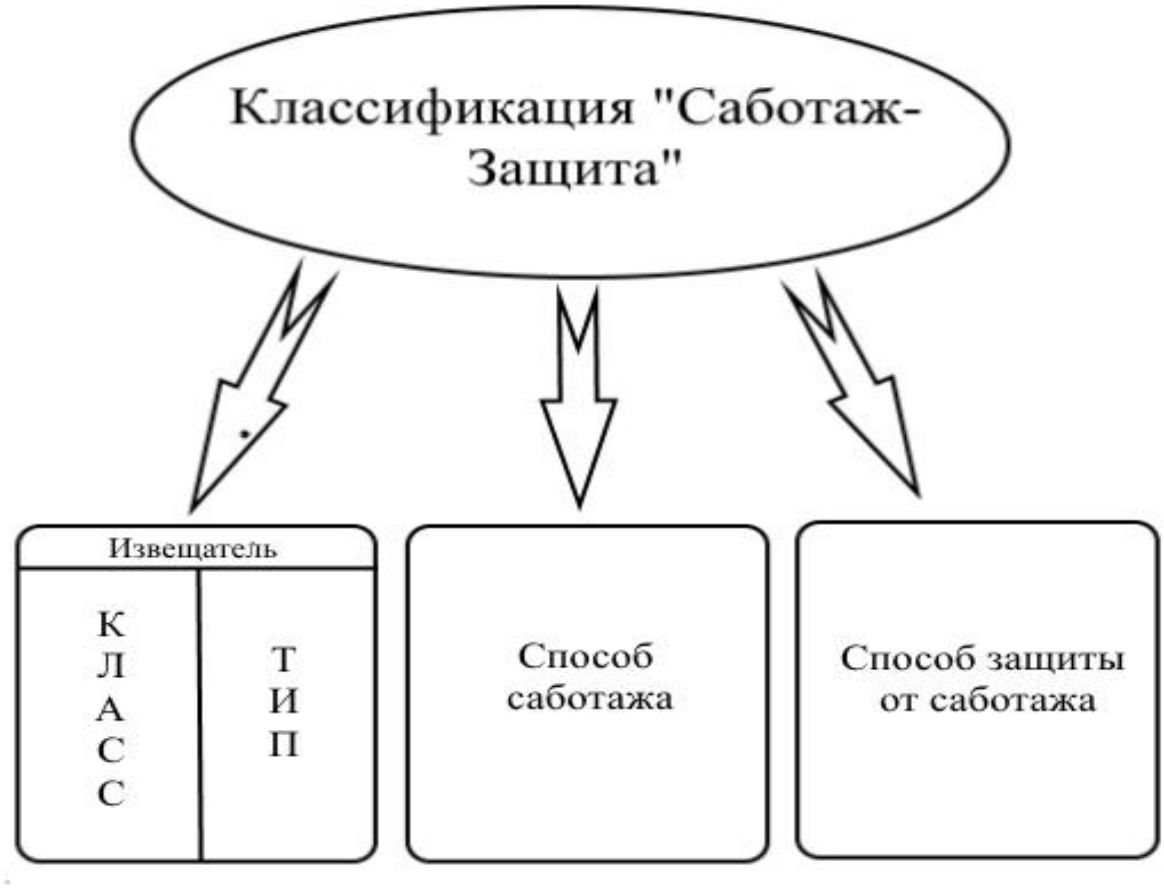


Рис. Структура классификации

Библиографический список

1. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов. Рекомендации (Р 78.36.028-2012). – М. : НИЦ «Охрана», 2012. – 359 с.

2. Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам. Рекомендации (Р 78.36.050-2015). – М. : НИЦ «Охрана», 2015. – 92 с.

3. Методическое пособие по выбору и применению пассивных оптико-электронных инфракрасных извещателей. Рекомендации (Р 78.36.036-2013). – М. : НИЦ «Охрана», 2013. – 195 с.

4. Большунов А. Г., Пузарин А. В., Захаров Д. Н. Теоретические основы утечки информации и защита телефонных переговоров // Технологии информационной безопасности в деятельности органов внутренних дел: сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 30-34.

5. Косачева И. Р., Пузарин А. В., Захаров Д. Н. Проблемы использования технических средств защиты информации от утечки по техническим каналам совместно с инновационными технологиями энергоснабжения // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 20–24.

6. Бегунков И. Д., Пузарин А. В., Захаров Д. Н. Программно-аппаратные средства защиты информации, передаваемой по техническим каналам связи // Технологии информационной безопасности в деятельности органов внутренних дел. Сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 69–70.

Д. Н. Саратов[1], *В. А. Редковников*[2]

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПРЕПОДАВАТЕЛЯ

В настоящее время весьма актуальной является проблема повышения эффективности учебного процесса в высшей школе. Ее решение невозможно без информатизации деятельности научно-педагогического состава. Внедрение современных информационных технологий позволит существенно сократить время, затрачиваемое преподавателями на методическую подготовку всех видов занятий, и повысить качество их проведения.

Опыт использования методов и средств информатизации производственной и социальной сфер показывает, что значительный эффект дает внедрение автоматизированных рабочих мест (АРМ) специалистов различных профилей. Применение этого подхода к педагогической деятельности определяет необходимость создания и последующего внедрения АРМ преподавателя. Такая работа ведется на кафедре специальных информационных технологий Санкт-Петербургского университета МВД России. Ожидается, что практическая реализация концепции АРМ преподавателя позволит снизить объем рутинной работы и повысить удельный вес творческого труда педагогов.

Традиционно АРМ определяется как индивидуальный комплекс технических, программных, информационных и других средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу (на экран и печать) необходимых документов и данных [1]. Необходимость использования АРМ в работе преподавателей определяется тем, что внедрение новых информационных технологий в практику проведения занятий требует разработки следующих видов учебно-методического обеспечения:

- учебники и учебные пособия, в том числе в электронном виде;
- тексты или конспекты лекций и презентации к ним;

---

[1] Заместитель начальника кафедры Специальных информационных технологий Санкт-Петербургского университета МВД России. © Саратов Д. Н., 2018.

[2] Начальник кабинета специальных дисциплин кафедры Специальных информационных технологий Санкт-Петербургского университета МВД России. © Редковников В. А., 2018.

– аудио- и видеоматериалы для интерактивных занятий;

– тестовые и оценочные материалы для промежуточных и итоговых контролей, в том числе в компьютерном исполнении;

– учебно-методическая документация (рабочие программы и тематические планы дисциплин, программы практик, методические рекомендации для подготовки к семинарским и практическим занятиям, методические рекомендации по самостоятельному изучению дисциплин и пр.) [2].

Научно-педагогический состав Санкт-Петербургского университета МВД России, в том числе, проводит занятия и по дисциплинам ограниченного доступа, относящимся непосредственно к деятельности полиции, в которых изучаются ведомственные руководящие документы. В данном случае особое внимание уделяется вопросам обеспечения защиты сведений, рассматриваемых в данных дисциплинах. В свою очередь это предполагает обеспечение информационной безопасности средств автоматизации преподавательской деятельности.

Основными направлениями обеспечения информационной безопасности АРМ преподавателя являются [3]: правовая защита; организационная защита; техническая защита; аппаратно-программная защита.

Первое направление заключается в создании такой нормативно-правовой базы, которая бы в полной мере обеспечивала защиту информации на правовой основе. Также к данному направлению относится совершенствование нормативно-правовых документов, регламентирующих защиту информации, в том числе Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 21.07.1993 г. № 5485-1 «О государственной тайне», Федерального закона от 29.07 2004 г. № 98-ФЗ «О коммерческой тайне», Доктрины информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).

Второе направление подразумевает регламентацию научно-педагогический деятельности сотрудников университета, использующих АРМ преподавателя. К основным механизмам осуществления данного направления можно отнести:

– разработку инструкций, регламентирующих правила и порядок работы научно-педагогического состава на АРМ при подготовке занятий, содержащих материалы ограниченного доступа;

– разработку локальной политики информационной безопасности подразделения (кафедры), в котором предполагается эксплуатация АРМ преподавателя.

– проведение с научно-педагогическими сотрудниками практических занятий, разъясняющих им основы работы на АРМ преподавателя.

Третье направление предполагает создание инженерных сооружений и применение технических средств, позволяющих обеспечить защищенность АРМ преподавателя от умышленных физических воздействий (намеренное повреждение или разрушение составных частей АРМ), а также обеспечивающих эксплуатацию АРМ в регламентированных условиях. Основными механизмами являются:

– установка АРМ преподавателя в категорированных помещениях;

– оборудование помещений системами контроля температуры и влажности воздуха, системами, обеспечивающими бесперебойную подачу электроэнергии, защиту от электромагнитных, вибрационных и ударных воздействий, а также автоматическими системами пожаротушения.

Четвертое направление предполагает применение систем защиты информации от несанкционированного доступа («Dallas Lock»), систем разграничения доступа к информации, а также криптомодемов и шифрующих (криптографических) программ.

Должное внимание следует уделить и системам дублирования и резервирования особо важной информации.

Таким образом, реализация и внедрение автоматизированных рабочих мест преподавателя с учетом обеспечения требований информационной безопасности позволят обеспечить автоматизацию преподавательской деятельности с высоким уровнем информационной защищенности.

Библиографический список

1. Примакин А. И. Использование автоматизированных рабочих мест в деятельности органов и учреждений Министерства внутренних дел Российской федерации [Текст] / А. И. Примакин, А. В. Муравьев, С. В. Селюгина // Вестник Санкт-Петербургского университета МВД России. – 2011. – № 4 (52). – С. 95–99.

2. Редковников В. А. Повышение эффективности педагогической деятельности преподавателя Санкт-Петербургского университета МВД России посредством автоматизации его рабочего песта [Текст] / А. Ю. Иванов, А. И. Примакин, О. Е. Чудаков, В. А. Редковников //

Вестник Санкт-Петербургского университета МВД России. – 2017. – № 1 (73) – С. 180–185.

3. Редковников В. А. Вопросы обеспечения информационной безопасности информационных систем органов внутренних дел Российской Федерации [Текст] // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 1-3 ноября 2017 г. : материалы конференции. – СПб. : СПОИСУ, 2017. – С. 68–70.

А. Ю. Кузнецов[1], Ю. Е. Богомолова[2]

PSYSCANNER – СОВРЕМЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ

Человеческий фактор всегда и везде был очень серьезной и не всегда разрешимой проблемой, а сейчас в силу того, что мы стали жить в мире, где обмен информацией становится основой существования общества, степень риска, связанная с безопасностью кадров, резко возросла.

Средний финансовый убыток от инцидентов, связанных с информационной безопасностью, резко увеличивается. Причем более половины инцидентов, зафиксированных в компаниях, связано с внутренними нарушителями и большую часть их составляют утечки информации, тут может быть как непреднамеренная утечка информации, допущенная по ошибке, так и умышленная, когда данные передаются конкурентам или копируются для последующего использования в личных целях.

Существующие способы анализа надежности человека, прогноза его поведения уже не удовлетворяют современным требованиям.

Психологические тесты, полиграфные проверки весьма трудозатратны, требуют высокого профессионализма сотрудника, который их проводит. При этом результаты проверок подчас находятся в прямой зависимости от опыта и субъективных качеств специалиста, а не от личностных качеств тестируемого.

---

[1] Генеральный директор Центра информационно-психологической безопасности, ассоциированный член Психологического института Российской академии образования. © Кузнецов А. Ю., 2018.

[2] Генеральный директор кадрового агентства Make Лайф (г. Москва). © Богомолова Ю. Е., 2018.

Для решения задач анализа надежности человека, прогноза его поведения нами был создан программно-аппаратный комплекс PsyScanner (далее – о АПК PsyScanner), который прошел верификацию (определение достоверности результатов) в Психологическом институте Российской академии образования на базе крупнейших коммерческих компаний, таких как Внешэкономбанк, ПАО Россети, Тинькофф банк и других.

Программно-аппаратный комплекс PsyScanner – это современная система, решающая задачи любой степени сложности, связанные с вопросами надежности и предсказуемости человека, определения его истинных мотивов, прогнозирования поведения и оценки отношения к тому или иному деянию, явлению или персоне.

АПК PsyScanner как полностью автоматизированная система предназначена для оперативного определения психологических особенностей и истинных мотивов поведения, прогнозирования степени надежности и предсказуемости, прогнозирования поведения и оценки отношения к тому или иному событию, явлению или персоне с возможностью документирования, углубленного анализа программ и автоматизированного обмена данными с удаленным пользователем с использованием сети Internet.

В период с 2007 по 2012 г. сотрудниками Центра информационно-психологической безопасности был разработан АПК PsyScanner. В основу действия АПК PsyScanner положен метод компьютерного нелокального психосемантического резонанса, который исключает сознательное восприятие тестируемым задаваемых вопросов, а также контроль выбора ответов.

В 2016 г. создан АПК PsyScanner с текстовым редактором и возможностью дистанционного тестирования по Internet.

Валидность АПК PsyScanner установлена в результате совместных научно-исследовательских работ с Психологическим институтом Российской академии образования на базе сборной команды Российской Федерации по лыжным гонкам, сборной команды Российской Федерации по гребле и ряда крупных коммерческих структур.

АПК PsyScanner реализует принцип нелокального психосемантического резонанса в системе человек – компьютер, прообразом которого являются синхронизм Юнга, резонанс Шумана, работы нобелевских лауреатов В. Паули и Д. Бома. В АПК PsyScanner используется метод предъявления, предложенный академиком И. В. Смирновым в 2002 г. (патент № 2218867 «Способ психозондирования»).

Создана трехуровневая система АПК PsyScanner для обеспечения кадровой безопасности:

– первый уровень – малый бизнес – тестирование проводится через личный кабинет, расположенный на сайте по стандартным программам;

– второй уровень – средний бизнес, по индивидуальному проекту заказчика составляется программа тестирования, к этой программе имеет доступ только представитель заказчика;

– третий уровень – большой бизнес, под каждую структуру разрабатывается свой АПК, который эксплуатируется непосредственно данной структурой.

Процесс тестирования происходит по следующему алгоритму:

– заказчик формирует задание на тестирование, т. е. основную тематику информации, которую он хотел бы получить и адрес электронной почты, на которую будут приходить протоколы тестирования;

– по этим данным составляется компьютерная программа;

– формируются и высылают заказчику логин и пароль для входа в программу;

– тестируемые в соответствии с инструкцией устанавливают програмmму тестирования на свой компьютер, введя логин и пароль входят в программу и проходят тестирование;

– после окончания тестирования результаты поступают на электронную почту Заказчика в виде текста или в виде графика (по согласованию);

– заказчик анализирует результаты тестирования и принимает соответствующее решение.

Смысл тестирования заключается в том, что программа замеряет скорость реакции тестируемого на неосознаваемые стимулы, заложенные в компьютерную программу. Программа регистрирует время реакции, а специальный математический аппарат программы преобразует полученные результаты в доступную для понимания и интерпретации форму-отчет в виде текста или гистограммы.

Достаточно авторитетными специалистами – полиграфологами В. Н. Федоренко и В. В. Коровиным был проведен сравнительный анализ методов детекции лжи и компьютерного психосемантического анализа (психозондирования), который выявил ряд преимуществ КПСА перед детектором лжи.

Сравнительная характеристика PsyScanner и Полиграфа

Полиграф	PsyScanner
Регистрация и запись физиологических параметров человека	Психосемантический анализ личности человека
Для проведения исследования необходимо специально подготовленное помещение и оборудование	Помещение не требуется. Тестирование проводится по Internet
Для проведения исследования требуется высококлассный специалист	Для проведения исследования специальных знаний не требуется
Подготовка исследования занимает около 2-х часов	Подготовка исследования из имеющихся тем занимает около 15 мин.
Возможно тестирование не более двух человек в день	Количество одновременно тестируемых не ограничено
Исследование возможно при условии, что специалист в совершенстве владеет языком испытуемого	Ограничений нет, можно проводить тестирование людей любой национальности
Время проведения первого исследования около двух часов по одной теме	Время проведения первого исследования около 25 мин. по 20 темам
Требуется подключение разнообразных датчиков	Подключение датчиков не требуется
Испытуемый информирован о теме исследования	Испытуемый не догадывается о содержании исследования
Исследование по той же теме не может быть повторено	Исследование по тем же темам возможно повторять ежедневно
Психофизиологическое состояние испытуемого оказывает влияние на результаты исследования	Психофизиологическое состояние испытуемого не оказывает влияние на результаты исследования (за исключением алкогольного и наркотического опьянения)
Испытуемый имеет возможность сознательно исказить результаты исследования, оказы-	Фальсификация результатов тестирования исключена

Полиграф	PsyScanner
вать противодействие	
Полученные результаты требуют интерпретации специалиста	Полученные результаты не требуют интерпретации специалиста

Резюмируя вышеизложенное, следует отметить, что АПК PsyScanner обладает за счет своих уникальных качеств:

– высокой достоверностью – не менее 85 % и невозможности фальсификации результатов;

– возможностью дистанционного тестирования по Internet;

– одновременный тестированием неограниченного числа людей;

– высокой производительностью: за 20 мин. тестируемый отвечает на 2000-2500 вопросов;

– простотой использования (протокол тестирования генерируется в виде текста) и т. д.;

– позволяет выводом системы кадровой безопасности компании на более качественно высокий уровень.

Раздел 3. ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ

Н. В. Лукашов[1]

О МЕЖВЕДОМСТВЕННОМ СИТУАЦИОННОМ ЦЕНТРЕ ПРОФИЛАКТИКИ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Термин «высокие технологии» (далее – ВТ) все чаще используется современной в юридической теории и практике. Его употребление естественным образом связано с технологическим развитием современной цивилизации. В юридической литературе укрепляется понятие, что этот термин «сложился стихийно для удобства обозначения преступлений, орудием или предметов которых стала компьютерная информация или компьютерные средства» [2]. То есть ВТ трактуются в узком смысле в качестве синонима компьютерным информационным технологиям (далее – ИТ).

Данную тенденцию подкрепляет отсутствие определенного соответствующего понятия в основных источниках права.

УК РФ содержит гл. 28 – «Преступления в сфере компьютерной информации», состоящую из трех статей: № 272 – «неправомерный доступ к компьютерной информации»; № 273 – «создание, использование и распространение вредоносных компьютерных программ»; № 274 – «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Ряд иных статей УК также содержат положения, связанные с компьютерной, в том числе финансовой информацией в качестве дополнительных квалифицирующих признаков (например, ч. 6 ст. 159 – «мошенничество в сфере компьютерной информации» и др.). Некоторые гражданско-правовые нормы направлены на регулирование правоотношений в сфере технологий и информации – право на топологии интегральных схем (гл. 74 ГК РФ), право использования результатов интеллектуальной деятельности в составе единой технологии (гл. 77) и др. Однако при этом термин ВТ явным образом нигде не фигурирует.

---

[1] Ведущий научный сотрудник отдела по исследованию стратегических проблем управления Научно-исследовательского центра Академии управления МВД России кандидат физико-математических наук, доцент. © Лукашов Н. В., 2018.

Анализ публикаций, учебно-методических материалов также показывает, что некоторые авторы если и разделяют понятия ВТ и информационные, компьютерные технологии (ИТ), то лишь в контексте разделения сложной технологической составляющей и информации, которая с ее помощью обрабатывается. Это находит отражение в локальных нормативных правовых актах правоохранительных органов. Так, инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола [4] в разделе «Информационное обеспечение борьбы с преступлениями в области высоких технологий» предусмотрено, что взаимодействующие органы направляют запросы о преступлениях в области высоких технологий, связанных с: «неправомерным доступом к компьютерной информации; созданием, использованием и распространением вредоносных программ для ЭВМ; нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети». Данная инструкция фактически ограничивает сферу ВТ сферой ИТ.

Между тем, вне сложившегося правового пространства правоохранительной деятельности, термин ВТ трактуется существенно шире и определяется, например, как «*совокупность информации, знаний, опыта, материальных средств, используемых при разработке, создании и производстве как новых (ранее неизвестных) продукций и процессов, так и для улучшения качества и удешевления производства известных продуктов*» [1].

В этом контексте, очевидно, что к ВТ относятся ядерные, космические, генетические, нано и ряд других технологий, не относящихся к ИТ, что и подтверждается практикой. Так, программой создания в России технопарков в сфере высоких технологий предполагается обеспечение ускоренного развития «таких высокотехнологичных отраслей экономики, как энергоэффективность и энергосбережение (в том числе разработка новых видов топлива), космические технологии (в том числе связанные с телекоммуникациями – ГЛОНАСС и наземная инфраструктура), медицинские технологии» [3].

Специфической особенностью расследования преступлений в сфере ВТ является характерная, в том числе и для сферы ИТ, расширенная практика привлечения специалистов и экспертов на всех стадиях уголовного процесса. Предъявляются повышенные требования к компетенции следователя (дознавателя) в предметной области расследования, что также связано с необходимостью проводить консультации со специалистами. При этом в ряде случаев круг носителей необходимых знаний может быть настолько узок, что найти независимого спе-

циалиста, не связанного с участниками процесса, может быть затруднительно или невозможно.

Также характерным общим признаком преступлений в сфере ВТ является их повышенная общественная опасность. Это позволяет поставить вопрос о совершенствовании квалификации преступлений и рассматривать использование ВТ в качестве отягчающего обстоятельства при совершении любых преступлений.

Специфика преступности в сфере ВТ заключается и в их «инновационности», использованием неизвестных ранее схем совершения преступлений, что обусловлено естественной новизной самих технологий.

В связи с этим можно обозначить ряд проблем, требующих безотлагательного решения. Среди них мы выделяем:

1. Необходимость нормативного закрепления понятия «высокая технология», которое при его интуитивной понятности требует глубокой теоретической проработки и философского осмысления. Основной признак ВТ – их сложность и оригинальность, недоступность для воспроизведения без специальных знаний, инструментов, материалов, а также в массе своей без глубокого разделения труда специалистов разного профиля.

2. Совершенствование, наработка методик расследования и квалификации преступлений в сфере ВТ на основе теории криминалистики и современной практики.

3. Формирование системы упреждающего реагирования и профилактики на вероятные угрозы для общества при совершении преступлений в сфере ВТ.

Это требует разработки особых подходов к процедуре их привлечения, а возможно и совершенствования ряда положений о статусе участников процесса.

Для повышения эффективности раскрытия, расследования и профилактики преступлений в сфере ВТ представляется целесообразным развитие коллективных (бригадных) методов работы. Это позволит свести к минимуму формализм во взаимодействии специалистов как на ведомственном, так и на межведомственном уровне. Такой способ систематически практиковался с участием автора в особых условиях на рубеже 1990-х годов и неизменно показывал чрезвычайно высокую эффективность. Так, количество проводимых ОРМ с использованием технических средств при наличии в составе бригады соответствующих специалистов и нормативных правовых оснований в 5-10 раз превы-

шало соответствующий показатель при организации аналогичных мероприятий на основе межведомственного и внутриведомственного взаимодействия отдельных служб. При этом существенно возрастали результативность и оперативность, а также снижалась трудоемкость подготовки и проведения.

Для расширения практики коллективных методов противодействия преступлениям в сфере ВТ необходимы единые регламенты взаимодействия, а также стандарты расследования, подготовки и проведения ОРМ, позволяющие снизить уровень внутриведомственной межведомственной разобщенности. Это позволило бы формировать оперативные группы с участием представителей разных специализированных служб под общим единым руководством, уполномоченным решать вопросы с привлечением их для выполнения соответствующих заданий напрямую, без трудоемкой процедуры согласования.

Одним из возможных путей организации такого взаимодействия может стать использование ситуационных центров или центров оперативного управления, развитие которых стало одним из трендов в ходе реформирования системы правоохранительных органов.

На базе таких ситуационных центров могли бы функционировать смешанные, в том числе межведомственные, оперативно-следственные группы, в составе которых сменами по 2–3 месяца, вахтовым методом, работали бы специалисты необходимых профилей. Срок привлечения специалистов может определяться средним временем раскрытия и расследования преступления (группы преступлений) до передачи дел в суд. Такой центр расследования преступлений в сфере ВТ (ЦРП) может иметь картотеку сотрудников и специалистов, обладающих необходимыми знаниями и навыками, привлекая их к работе на плановой (посменной) или, при крайней необходимости, внеплановой основе.

В свою очередь специалисты, перенимая передовой опыт работы в ЦРП, могут стать проводниками для его распространения в своих базовых подразделениях. Очевидно, такой Центр помимо методических функций должен осуществлять прогнозирование, а также разработку мер по превентивному реагированию и профилактике преступности в сфере ВТ.

Таким образом, противодействие новому виду преступлений, характерному для современного этапа развития общественных отношений, может и должно осуществляться на основе новых принципов организации выявления, раскрытия и расследования преступлений.

Библиографический список

1. Большая Российская энциклопедия: – М. : Большая Российская энциклопедия: в 30 томах. – Т. 6.
2. Кушниренко С. П. Методика расследования преступлений в сфере высоких технологий. Конспект лекций С. П. Кушниренко; СПб.: Юрид. ин-т Генеральной прокуратуры Российской Федерации. – СПб., 2007.
3. Распоряжение Правительства Российской Федерации от 10.03.2006 № 328-р (ред. от 29.11.2014 г.) «О государственной программе «Создание в Российской Федерации технопарков в сфере высоких технологий».
4. Приказ МВД России № 786, Минюста Российской Федерации № 310, ФСБ Российской Федерации № 470, ФСО Российской Федерации № 454, ФСКН Российской Федерации № 333, ФТС Российской Федерации № 971 от 06.10.2006 (ред. от 22.09.2009 г.) «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

Д. Б. Родионова[1], А. С. Овчинский [2]

ПРОФИЛАКТИКА ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В ЦИФРОВОМ МИРЕ

Общесоциальная и оперативно-разыскная профилактика преступлений террористической и экстремистской направленности. Экстремизм и терроризм в настоящее время являются реальной угрозой национальной безопасности. Вступление в цифровой мир со стремительным развитием интернет-коммуникаций, большими данными и искусственным интеллектом открывают качественно новые возможности не только в практике противодействия терроризму и экстремизму, но и в системной профилактике этих антисоциальных явлений.

Известно, что оперативно-разыскная профилактика предполагает сбор информации о криминально-активных лицах (членах организованных преступных формирований, ранее судимых, распространителях наркотиков, бытовых дебоширах, членах групп с антиобществен-

---

[1] Слушатель 518 учебного взвода 5 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Родионова Д. Б., 2018.

[2] Профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя доктор технических наук, профессор. © Овчинский А. С., 2018.

ной направленностью и др.), их связях, преступном опыте, намерениях, особенностях их личностных качеств и антисоциальных проявлениях [1].

Из теории и практики ОРД следует, что совокупность сведений, которые дают основания для неблагоприятного прогноза, т. е. вывода о вероятности преступного поведения, может указывать на необходимость установления оперативного наблюдения за теми, кто проявляет криминальную активность.

При осуществлении мер оперативно-разыскной профилактики применяется особая тактика получения и использования оперативно-разыскной информации. Сложились и своеобразные организационные формы. Осуществление оперативно-разыскной профилактики требует привлечения знаний из области криминологии и педагогики, умения прогнозировать развитие криминогенной ситуации и индивидуального преступного поведения.

Специфичность оперативно-разыскной профилактики заключается в следующем:

– ведется оперативно-профилактическое наблюдение за лицами, поставленными на профилактический учет в связи с высокой степенью вероятности их преступного поведения;

– фиксируется среда местных криминально активных жителей, в которой осуществляются оперативно-разыскные мероприятия по раскрытию преступлений;

– негласно проверяется причастность к совершенным преступлениям лиц (в том числе и ранее выявленных не местных жителей), находящихся под оперативным наблюдением и имеющих признаки разыскиваемых преступников;

– изучаются отдельные категории лиц, представляющих оперативный интерес, их связи, образ жизни, поведение и прошлое для получения оснований к применению мер профилактики или для заведения дел оперативного учета;

– обеспечивается успех индивидуальной профилактики благодаря оперативной осведомленности о контингенте лиц, которые могут встать на путь совершения преступлений, и особенностях каждого лица, допустившего антиобщественное поведение или испытавшего вредное влияние антиобщественных и преступных элементов [2].

Сочетание целей профилактики с постоянной проверкой лиц, находящихся под оперативно-профилактическим наблюдением, проведением среди них ОРМ для обнаружения преступников является специ-

фическим признаком оперативно-разыскной профилактики. Такое сочетание обеспечивает оперативную осведомленность о контингенте лиц, относимых к категории криминально активных, позволяет своевременно прибегать к оперативной разработке преступников с использованием всех материалов, собранных при осуществлении мер оперативно-разыскной профилактики. Каждый из элементов оперативно-разыскной профилактики может стать частью сложной процедуры получения оснований для оперативной разработки. Причем соотношение этих элементов оперативно-разыскной профилактики определяется складывающейся оперативной обстановкой [3].

В рамках оперативно-разыскной профилактики получают и используют сведения об условиях, способствующих совершению преступлений. Часто негласные сотрудники сообщают о фактах нарушений норм нравственности, подогревании враждебных отношений между людьми на национальной и религиозной основе и прочих негативных явлениях, которые способствуют антиобщественному и преступному поведению. Такая информация не всегда может быть реализована без предварительного документирования и принятия мер к зашифровке ее источников. Но после принятия таких мер она может быть использована в методах уже общей профилактики, которая предполагает:

– устранение условий, способствующих формированию личности правонарушителя (террориста, экстремиста);

– устранение возможности возникновения острых конфликтных ситуаций в отношениях между людьми;

– устранение условий, облегчающих совершение преступлений на конкретных объектах;

– исключение посягательств на общественный порядок и личность граждан в общественных местах.

Терроризм и экстремизм в информационных сферах. Социальная и материальная незащищенность молодежи, частый максимализм в оценках и суждениях, психологическая незрелость, значительная зависимость от чужого мнения – вот только некоторые из причин, позволяющих говорить о возможности легкого распространения радикальных идей среди российской молодежи. Лидеры экстремистских группировок различного толка завлекают молодежь в свои объединения, часто обещая ей легкое решение всех проблем, в том числе и материальных. Неокрепшие молодые умы зачастую даже не задумываются о том, что, участвуя в деятельности подобных формирований, они не только не решают свои существующие проблемы, но и создают

себе многочисленные новые, по сути, уничтожают свое будущее. Безусловно, проводить, как общесоциальную, так и оперативно-разыскную профилактику экстремизма и терроризма среди молодежи намного эффективнее, чем ликвидировать последствия подобных явлений [4].

Наиболее эффективным средством массового информационного воздействия террористов на молодежь в последнее время становится Интернет. Причины популярности Интернета в преступной среде – легкий доступ к аудитории, обеспечение анонимной коммуникации, слабое регулирование на государственном уровне, глобальное распространение, высокая скорость передачи информации, дешевизна и простота в использовании, мультимедийные возможности.

Экстремистские ресурсы широко используют средства психологической войны, в том числе дезинформацию, запугивание, манипуляцию общественным сознанием, подмену понятий и фактов. На интернет-ресурсах террористических организаций освещается психологический ущерб, наносимый государствам-объектам атаки в результате терактов.

Террористические организации используют Интернет для вербовки новых членов, включая террористов-смертников из числа как исламистов, так и экстремистски настроенной молодежи. Привлечение в радикальный ислам переходит в противоправную деятельность. Кроме того, Интернет используется для формирования «лояльно настроенной среды», играющей активную роль в поддержке экстремизма и террористических организаций [5].

В настоящее время во всемирной сети представлены практически все типы организаций, применяющих в своей деятельности экстремистские и террористические методы. Число сайтов, содержащих материалы экстремистского характера, превышает семь тысяч, среди них более ста пятидесяти русскоязычных. Спецслужбами и правоохранительными органами фиксируется использование идеологами террористических организаций все новых и новых средств коммуникации для наибольшего охвата аудитории. Так, параллельно с развитием сервисов мобильной связи делаются доступными скачивание экстремистской литературы на мобильный телефон, соответствующие E-mail, MMS и SMS-рассылки и т. д. [6].

Наряду с использованием новейших информационных технологий экстремистскими и террористическими организациями в целях вербовки молодежи также задействуются и традиционные каналы соци-

ального взаимодействия. Значительным идеологическим ресурсом экстремистов, террористов и бандподполий является обучение молодых граждан России в зарубежных теологических учебных заведениях. Основная категория обучающихся – молодые люди в возрасте 20-25 лет.

Информационно-технологическое обеспечение профилактики терроризма и экстремизма. Для борьбы с этими негативными тенденциями органы государственной власти, местного самоуправления с привлечением возможностей гражданского общества должны сосредоточить свои усилия на следующих направлениях информационно-технологического, информационно-аналитического и информационно-психологического обеспечения профилактики терроризма и экстремизма:

– информационно-аналитическое обеспечение (выпуск памяток, брошюр, книг, обращений, плакатов, социальной рекламы, создание тематических документальных фильмов и видеороликов и т. д.);

– пропагандистское обеспечение (своевременное доведение объективной информации о результатах деятельности правоохранительных органов и спецслужб в борьбе с экстремизмом и терроризмом);

– контрпропагандистское обеспечение (адекватная и своевременная реакция на дезинформацию, выступления, высказывания главарей бандформирований, распространение листовок и пропагандистской литературы);

– идеологическое обеспечение (формирование религиозной и межнациональной терпимости, патриотизма, здорового образа жизни, приоритетов общечеловеческих ценностей и т. д.);

– организационное обеспечение (содействие деятельности общественных и религиозных объединений традиционной конструктивной, в том числе антитеррористической; направленности; взаимодействие со СМИ, проведение конференций, слетов, «круглых столов», конкурсов на лучшие материалы антитеррористического характера и т. д.);

– образовательное обеспечение (создание системы подготовки специалистов, в том числе из числа гражданских лиц, в области информационного противодействия терроризму). Подобную работу следует вести наступательно, в том числе отстаивая интересы России в этой области на международном уровне [7].

По данным Национального антитеррористического комитета, в регионах России активно формируются кибердружины – сообщества

молодых людей, стремящихся противостоять экстремистскому контенту. Создан Национальный центр информационного противодействия терроризму. Опыт сотрудничества общественных организаций с правоохранительными и правоприменительными органами позволяет сформулировать ряд перспективных направлений работы в области информационного противодействия экстремистскому контенту в сети, которые направлены и на профилактику терроризма:

– привлечение общественности (краудсорсинг) для выявления фактов пропаганды радикальных идей, сбора средств и др. (создание «горячих линий», комфортных для сбора жалоб от различных социальных групп граждан);

– привлечение общественности к процессу частичного ограничения доступа к радикальным материалам в сети «Интернет» (активно используется на сайте НЦПТИ при помощи сервиса: «Сообщить о противоправном контенте»);

– создание и периодическое обновление площадок распространения профилактической литературы в электронном виде (решение проблемы дефицита профилактической литературы в регионах, отслеживать распространение результатов новейших исследований;

– создание механизма «обратной связи» для целевых аудиторий, которой предназначена профилактическая литература (повышение позволит повысить эффективности разрабатываемых специалистами материалов) [8].

Основная цель профилактики в противодействии терроризму и экстремизму – помочь молодым людям развить в себе сильную социально-активную и ответственную личность, выработать жизненную позицию, способную противостоять факторам риска.

Библиографический список

1. Теория оперативно-разыскной деятельности; учебник / под ред. К. К. Горяинова, В. С. Овчинского – 4-е изд., перераб. и доп. – М. : ИНФРА-М, 2018.

2. Овчинский С. С. Оперативно-разыскная информация: монография // под ред. А. С. Овчинского, В. С. Овчинского. 2-е изд., доп. – М. : ИНФРА-М, 2017.

3. Бабушкин А. А. Правовые вопросы формирования системы оперативно-разыскного контроля за лицами, склонными к совершению преступлений // Актуальные проблемы оперативно-разыскной деятельности: сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. – М. : ИНФРА-М, 2017.

4. Овчинский А. С. Оперативно-разыскная аналитика на пути к искусственному интеллекту // Актуальные проблемы оперативно-разыскной деятельности: сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. – М. : ИНФРА-М, 2017.

5. Овчинский А. С. Оперативно-розыскная аналитика (ответ современным угрозам): монография. – М. : Издательский дом И. И. Шумиловой, 2015.

6. Осипенко А. Л. Оперативно-разыскная деятельность в период четвертой промышленной революции // Актуальные проблемы оперативно-разыскной деятельности: сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. – М. : ИНФРА-М, 2017.

7. Овчинский В. С. Использование искусственного интеллекта в оперативно-аналитической деятельности ФБР по борьбе с преступностью // Актуальные проблемы оперативно-разыскной деятельности: сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. – М. : ИНФРА-М, 2017.

8. Чурилов С. А., Быкадорова А. С. О противодействии распространению и профилактике радикальных идеологий в молодежной среде и сети «Интернет». Статья. cyberleninka.ru.

***В. В. Прудиус*[1], *Е. М. Шпагина*[2]**

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ СБОРА ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ

В настоящее время количество социальных сетей (таких как «Одноклассники», «ВКонтакте», «МойМир», «МойКруг», «МирТесен», MySpace) в Интернете и численность их участников растет с невероятной быстротой. Социальные сети сегодня уже посещает более чем две трети онлайн-аудитории во всем мире, и это четвертая по популярности онлайн-категория после поисковых порталов, информационных порталов и программного обеспечения, которая опережает даже электронную почту (по данным компании Nielsen Online, исследующей онлайн поведение в 9 странах). По данным той же компании, исполь-

[1] Слушатель 518 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Прудиус В. В., 2018.

[2] Начальник кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя, кандидат психологических наук. © Шпагина Е. М., 2018.

зование онлайн-сообществ сегодня растет вдвое более быстрыми темпами, чем любой из четырех других секторов сети «Интернет» и в три раза быстрее, чем пользование Интернетом в целом.

Социальные сети (social networks) привлекают людей, преследующих различные цели: поддержание контакта со старыми знакомыми и поиск новых, в том числе обустройство личной жизни; поиск работы, продвижение своего бизнеса, профессиональное общение; обмен информацией и медиаконтентом с другими пользователями. Аудитория различных социальных сетей сильно отличается друг от друга. Так, пользователей в возрасте от 15 до 24 следует искать в сети «Мой Мир» на Майл.ру, от 16 до 34 – в сети «ВКонтакте», а от 20 до 53 – в сети Одноклассники.ру.

В России социальные сети появились сравнительно недавно, хотя довольно давно распространены за рубежом. Но, несмотря на это, некоторые из них приобретают огромную популярность, другие же с большим успехом составляют им конкуренцию. Основные дискуссии развиваются около вопроса: чем являются социальные сети «Интернет» для современного человека – злом или благом?

Использование методов социальной инженерии для вхождения в доверие подозреваемого. В решении задач информационной безопасности человеческий фактор занимает одну из важнейших позиций. Еще несколько лет назад подавляющее большинство всех несанкционированных доступов (НСД) к информации совершались с использованием технических средств. Ситуация изменилась, и на смену техническим средствам пришла социальная инженерия.

Технологии безопасности, которые бурно развивались последнее время (межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и другие) оказались малоэффективными в противостоянии хакерам, использующим методы социальной инженерии. Социальная инженерия (англ. – social engineering) – это способ совершения преступлений в сфере компьютерной информации с использованием комплекса приемов, не имеющих отношения к программно-аппаратным методам НСД, совершаемых с использованием познаний в области психологии.

Специалисты в области информационной безопасности долгое время обращали внимание только на аппаратные и программные средства защиты, однако этого стало недостаточно. Кроме данных способов защиты, необходима серьезная работа с персоналом, обучение сотрудников применению политики безопасности и техники противо-

стояния социоинженерам – только в этом случае система обеспечения информационной безопасности будет комплексной.

В совокупности с техническими познаниями в области информационной безопасности социальная инженерия представляет собой очень серьезное оружие. В области компьютерных преступлений ее используют для достижения следующих целей:

1. *Сбор информации о потенциальной жертве*. Приведем пример: злоумышленник обладает исключительно общей информацией о жертве, но для достижения каких-либо результатов ему необходимо обладать некоторой конкретной информацией о жертве. В этом случае злоумышленник, например, вступает в диалог (переписка, разговор в службах обмена быстрыми сообщениями (messenger), например, ICQ) сначала с теми, кто непосредственно общается с жертвой, затем и с самой жертвой. Из подобного рода общения злоумышленник может без проблем узнать конкретную информацию о жертве, такую как время появления в сети «Интернет», интересы, особенности поведения, предпочтения, вкусы, увлечения, территориальное месторасположение, часто посещаемые ресурсы (например, форумы), имена, под которыми жертва появляется в сети «Интернет» и даже тип операционной системы, используемой жертвой.

По этим данным злоумышленник может спланировать дальнейшие действия, направленные на получение НСД.

2. *Получение конфиденциальной информации*. Для достижения данной цели злоумышленник при продолжительном общении с жертвой входит в доверие и под удобными предлогами получает необходимую информацию (например, получить пароли от почтовых аккаунтов). После вхождения в доверие к жертве злоумышленник может узнать реальное имя и фамилию жертвы.

Затем воспользоваться этими сведениями для получения остальной необходимой информации (например, используя базы данных, вычислить номера телефонов жертвы, адрес прописки/проживания и многое другое вплоть до информации о жертве, как о налогоплательщике).

3. Получение информации, необходимой для НСД. Жертва имеет аккаунт на одном из публичных почтовых серверов (таких как mail.ru, yandex.ru и т. д.). На любом из них присутствует «Служба восстановления пароля». Эта служба существует для того, чтобы пользователи могли восстановить свой пароль при его утере. Для этого при регистрации они обычно вводят специальный вопрос, ответ на который является однозначной аутентификацией пользователя. Чаще всего ис-

пользуются такие вопросы, как «Девичья фамилия матери», «Ваше любимое блюдо» или «Серия и номер паспорта». Таким образом, если пользователь забыл свой пароль, он обращается в автоматизированную службу его восстановления, правильно отвечает на вопрос и получает новый пароль для доступа к своему почтовому аккаунту.

Для достижения данной цели злоумышленник обращается к автоматической службе восстановления пароля и узнает контрольный вопрос. Допустим, вопросом является «Ваше любимое блюдо». Далее злоумышленник входит в доверие к жертве и предлагает провести встречу «в живую». Далее злоумышленник под разными предлогами (встреча в ресторане, предпочтения в домашней кухне и т. д.) получает перечень кулинарных предпочтений жертвы.

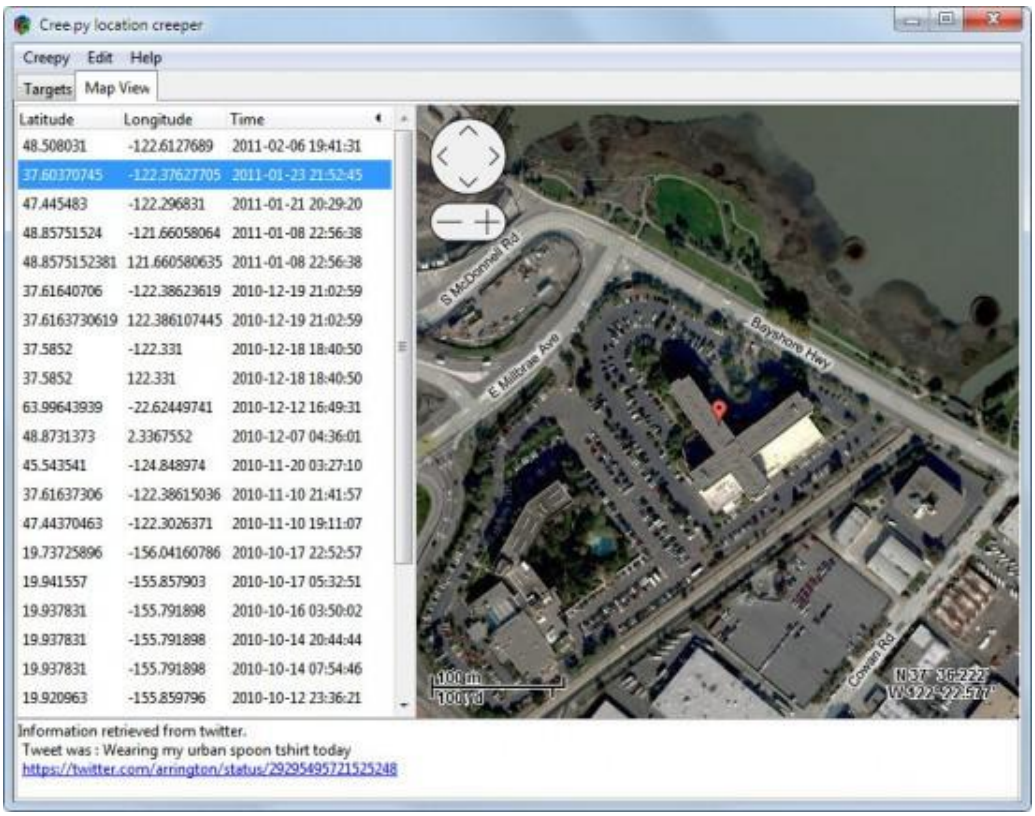
После этого злоумышленник с высокой степенью вероятности правильно отвечает на контрольный вопрос службы восстановления пароля. Или же, если контрольный вопрос звучит как «Серия и номер паспорта», злоумышленник узнает реальное имя, отчество и фамилию жертвы, после чего по нелегально добытым, однако находящимся в свободной продаже на компьютерных рынках базам данных вычисляет серию и номер паспорта жертвы.

Существует несколько бесплатных утилит, позволяющих вытаскивать информацию о пользователях из социальных сетей.

Одна из наиболее популярных – Сгееру. Она предназначена для сбора геолокационной информации о пользователе на основе данных из его аккаунтов Twitter, Instagram, Google+ и Flickr [2].

Все, что вам нужно сделать, –это ввести имя пользователя Flickr или Twitter в приложение и подождать, пока оно извлечет информацию о долготе и широте. Добавляете время размещения поста плюс интеграция с Google Maps, Virtual Maps и Open Street Maps и вы создали перемещения профиля данного пользователя. Твит и URL твита, или название изображения и ссылки в Flickr, размещаются в окне внизу программы для каждого хита.

FbStalker и GeoStalker. FbStalker предназначен для сбора информации о пользователе на основе его Facebook-профиля. Позволяет выцепить следующие данные: видео, фото, посты пользователя; кто и сколько раз лайкнул его записи; геопривязки фоток; статистика комментариев к его записям и фотографиям; время, в которое он обычно бывает в онлайне.



GeoStalker значительно интереснее. Он собирает информацию по координатам, которые ты ему передал. Например: местные Wi-Fi-точки на основе базы `wigle.net` (в частности, их `essid`, `bssid`, `geo`); чекины из Foursquare; Instagram- и Flickr-аккаунты, с которых постились фотки с привязкой к этим координатам; все твиты, сделанные в этом районе.

Библиографический список

1. Батура Т. В. Методы анализа компьютерных социальных сетей // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2012. – Т. 10. № 4. – С. 13–28.

2. Прудиус В. В., Захаров Д. Н., Прудиус В.В. Использование социальных сетей для сбора информации о пользователях // Сборник трудов XV научно-практической конференции «Технологии информационной безопасности в деятельности органов внутренних дел». – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 151–156.

Е. В. Клянчина[1], ***А. Д. Распутина***[2]

ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ: АСПЕКТЫ ИСПОЛЬЗОВАНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Первостепенная задача, стоящая перед органами внутренних дел, – это «защита жизни, здоровья, прав и свобод граждан, собственности и интересов общества и государства от преступных и иных противоправных посягательств» [1].

Для решения этой задачи необходимо наличие эффективного информационно-аналитического обеспечения управленческих функций, связанных с прогнозированием и планированием, регулированием и координацией, учетом и контролем деятельности структурных подразделений органов внутренних дел.

В рамках совершенствования правоохранительной деятельности, в том числе связанного с наращиванием средств автоматизации работы ОВД, широкое распространение в практической деятельности силовых структур находят информационные технологии и методы, позволяющие обрабатывать большое количество информации, имеющей географическую привязку к земле, так называемую геоинформацию, – данные о состоянии преступности на территории оперативного обслуживания территориальных органов полиции, о криминальной ситуации в масштабах региона или субъекта, территориальной инфраструктуре органов внутренних дел, кадровом обеспечении регионов, возможных террористических угрозах, логистических маршрутах специальных охраняемых грузов, режимных объектах, расстановке и маршрутах передвижения нарядов патрульно-постовой службы, организации и регулировании дорожного движения.

Следует отметить фактор геомасштаба организационной иерархии ОВД: чем ближе к земле (ниже уровень иерархии ОВД), тем больше количество обрабатываемой геоинформации, шире ее номенклатура, выше темп поступления и изменения. В связи с этим абсолютно оправдано применение в органах внутренних дел для обработки больших геоинформационных массивов специальных современных средств –

---

[1] Преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Клянчина Е. В., 2018.

[2] Курсант 336 учебного взвода 3 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Распутина А. Д., 2018.

геоинформационных технологий (ГИТ) и геоинформационных систем (ГИС), позволяющих искать, собирать, хранить, анализировать и географически визуализировать пространственные данные и связанную с ними дополнительную информацию об интересующих объектах.

Использование геоинформационных систем напрямую связано с процессом геоинформационного анализа, который в свою очередь является частью аналитической деятельности человека. Сбор данных из подходящих источников требует опыта в их подборе, независимо от того, насколько окончательный процесс сбора данных может быть автоматизирован. Для превращения собранных данных в аналитические выводы и эффективного применения их на практике необходимы знания в области геоинформатики и наличие навыков аналитика.

В процессе анализа геоинформации можно условно выделить несколько этапов:

– определение цели и объема поставленной задачи по геоинформационному анализу;

– сбор информации из первичных источников;

– использование вторичных источников информации;

– оценка полученных данных: проведение реферирования информации, собранной из различных источников, и выделение тех данных, которые необходимы для первоначального анализа в соответствии с поставленной задачей;

– проведение аналитических мероприятий;

– предоставление результатов и подготовка отчета (аналитической справки) – этап, на котором немаловажное значение имеет формат представления конечного результата исследования, выбранные аналитиком средства и способы визуализации полученных данных и сделанных выводов, в том числе с использованием географических карт, схем местности и т. д.

– использование результатов проведенного анализа – этап, на котором оценивается успешность выполнения поставленной задачи, дается оценка полученных данных и сделанных выводов с точки зрения их практического применения.

Для эффективного использования геоинформационных средств и технологий в ОВД требуется разработка специальных или адаптация существующих ГИС, учитывающих специфику предметной области и решаемых полицией задач. Все программное обеспечение ГИС можно условно разделить на три класса: Web-ГИС, настольные ГИС, пространственные базы данных.

Настольные или пользовательские ГИС представляют собой картографическое программное обеспечение, предназначенное для установки и запуска на персональном компьютере, позволяющее отображать, выбирать, обновлять и анализировать данные о географических объектах и связанную с ними атрибутивную информацию.

Среди существующих ГИС можно выделить следующее программное обеспечение зарубежных разработчиков: Geographic Resources Analysis Support System (GRASS), Quantum GIS (QGIS), User-friendly Desktop Internet GIS (uDig), Generalitat Valenciana, Sistema d'Informacio Geografica (gvSIG), System for Automated Geoscientific Analyses (SAGA), MapWindow GIS, Integrated Land and Water Information System (ILWIS) [2].

Изучив основные характеристики, функционал и особенности работы вышеперечисленных ГИС, можно говорить о том, что наиболее эффективно в аналитической работе органов внутренних дел может быть использована геоинформационная система QGIS, т. к. она обладает отличной совместимостью со средой разработки, картографическими данными, а также позволяет настраивать свои функции под любые геоинформационные задачи.

Синтез геоинформационных технологий и сведений о преступлениях и иных правонарушений позволяет создать особое информационно-аналитическое пространство, способное предоставить целый ряд преимуществ перед ныне действующими методами информационно-аналитического обеспечения деятельности ОВД по профилактике правонарушений.

Вместе с тем, на основе изучения опыта использования информационных технологий визуализации данных в правоохранительной деятельности и проведенного сравнительного анализа программного обеспечения ГИС можно сформулировать основные характеристики, присущие функционалу и возможностям ГИС, используемым в целях осуществления качественного информационно-аналитического обеспечения деятельности органов внутренних дел, а именно:

1. Возможность ГИС наиболее полно сосредоточить информацию в едином пространстве, что окажет положительное влияние на результаты решения специальных задач, в том числе связанных с организацией и проведением оперативно-разыскных мероприятий, действиями при чрезвычайных обстоятельствах или чрезвычайных ситуациях, а также контрольными функциями.

2. Возможность наглядно оценивать складывающуюся обстановку состояния преступности на обслуживаемой территории в целях рационального использования сил и средств, точечно воздействуя на пораженные участки местности интенсивными профилактическими мерами.

3. Возможность автоматизировать процесс анализа и прогноза преступных проявлений в пространственно-временном измерении с выделением факторов местности, способных служить причинами совершения преступлений.

Таким образом, среди основных направлений деятельности ОВД, где использование ГИС и ГИТ является оправданным и эффективным, следует отметить управление ведомственными силами и средствами; планирование профилактики преступлений и правонарушений на отдельно взятой территории оперативного обслуживания ОВД; анализ оперативной обстановки, позволяющий оценить особенности конкретных территорий в масштабах страны, субъекта, города или района; планирование проведения оперативно-разыскных мероприятий, в том числе в отношении преступных групп и сообществ, преступная деятельность которых растянута во времени и пространстве; осуществление аналитических мероприятий по отдельным видам преступлений (тематических исследований) на территории отдельно взятого региона, например, «геоинформационный мониторинг террористической деятельности в России» [3].

В целом, использование геоинформационных систем и методов геоинформационного анализа в ОВД позволит повысить рациональность принимаемых управленческих решений, эффективность мероприятий, направленных на сбор, обработку, хранение информации, представляющей оперативный интерес, а также на качество представления и визуализации данных в процессе информационно-аналитического обеспечения правоохранительной деятельности в целом.

Библиографический список

1. Федеральный закон Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции».

2. Середкина О. М. ГИС-технологии в изучении распределения радона на территории города Иркутска : дис. … Иркутск, 2012. – Электронная библиотека РГБ, библиотека диссертаций – http://diss.rsl.ru.

3. Супрунчук И. П. Концепция функционирования ГИС «Террористическая деятельность в России» // Вестник Северо-Кавказского федерального университета. – 2014. – Вып. 3 (42).

О. С. Биккулова[1]

АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: СИСТЕМА «ЛКС АНАЛИТИКА»

Современные пользователи сети «Интернет» имеют доступ к большим объемам открытой информации. Широкая доступность и высокая скорость получения необходимой информации оказывают положительное влияние на профессиональную, научную и учебную деятельность. Обратной стороной обилия разнородной информации является невозможность качественного поиска нужных материалов среди информационного шума. С возрастанием объема информации поиск самой значимой и даже критически важной информации занимает все больше времени.

Система «ЛКС Аналитика» – это решение для автоматического мониторинга СМИ, социальных медиа и различных открытых источников сети «Интернет». Она была разработана для автоматизации и улучшения качества работы аналитика. Благодаря тотальному сбору и точному анализу входящего потока сообщений система «ЛКС Аналитика» позволяет:

– проводить качественный мониторинг текстовой информации 24 часа в сутки, семь дней в неделю;

– исключить «человеческий фактор» и пропуск целевого сообщения;

– сократить временные и трудовые затраты на поиск, систематизацию и визуализацию информации.

Схема работы системы. Система «ЛКС Аналитика» состоит из нескольких модулей, которые настраиваются под конкретные задачи поиска и анализа информации. Общая схема работы модулей состоит из трех этапов:

Этап 1. Сбор сообщений из сети «Интернет».

Этап 2. Систематизация информации с помощью семантических фильтров и специальных алгоритмов.

Этап 3. Визуализация структурированной информации, работа пользователя, подготовка отчетов.

---

[1] Компьютерный лингвист ООО «Компьютерные системы ЛКС». © Биккулова О. С., 2018.

Система имеет возможности гибкой настройки на поиск конкретных типов сообщений: подключение новых источников, корректировка лингвистических алгоритмов и настройка семантических фильтров. Поэтому за более чем 20 лет работы системы и ее модификаций «ЛКС Аналитика» была успешно опробована в качестве инструмента превентивного мониторинга различных угроз безопасности.

Примеры задач

1. Мониторинг угроз объектам инфраструктуры. Трудности обеспечения безопасности инфраструктурных объектов заключаются в удаленности объектов друг от друга и их многочисленности. Инструментом одновременного контроля за несколькими объектами является система мониторинга открытой информации. Успешно опробована работа системы «ЛКС Аналитика» для отслеживания ситуации вокруг гидроэлектростанций, находящихся в разных точках России. Технологии мониторинга позволяют собирать информацию из любых географических точек страны и мира. Поэтому для мониторинга за важными энергетическими объектами на территории Российской Федерации система «ЛКС Аналитика» была настроена таким образом, что в базу данных агрегировалась информация не только из центральных и региональных СМИ, но из специфических источников: сайты сейсмической активности Земли (в основном англоязычные), сайты прогнозов погоды, сводки криминальных новостей в регионах, социальные сети, форумы и блоги туристов, спелеологов и «экстремалов» в каждом регионе присутствия. Таким образом, аналитик в едином Центре мониторинга получил доступ ко всей информации, которая могла быть значима для ежедневной работы гидроэлектростанции. По отзывам аналитиков департамента безопасности система помогла получать критические сообщения раньше, чем сотрудники на самом объекте.

2. Мониторинг протестной активности. Другим примером обеспечения аналитической деятельности с помощью мониторинга является отслеживание общественных дискуссий в Интернете, которые впоследствии могут вылиться в митинги и протестные акции. Кроме непосредственных сообщений в социальных сетях, содержащих активные призывы к пикету или уличной демонстрации, «ЛКС Аналитика» может вычленять проблемные «негативные» вопросы, которые только начинают подниматься на форумах и в социальных сетях. Например, длительный конфликт местных жителей и верующих в парке Торфянка прошел все стадии, которые можно было наблюдать и предсказать в системе мониторинга: от зарождения конфликта до уличных столкно-

вений. В данный момент система с помощью настроенных семантических фильтров может вычленять из информационного потока мнения сторонников и противников конфликта. На основе разделения на «за», «против» и остальной информации можно не только быть в курсе конфликтной ситуации, но и строить качественную аналитику, а в дальнейшем, например, прогнозировать количество людей, которые придут на митинг.

3. Борьба с компьютерными угрозами. По данным Лаборатории Касперского, в 2016 г. 77 % компаний неоднократно испытывали на себе действие DDoS-атак. 315 тыс. вредоносных программ появляются в сети ежедневно. Количество семейств вредоносных программ выросло за 2016 г .в 8,5 раз, т. е. компьютерные угрозы становятся все изощреннее [3].

Часть угроз можно нейтрализовать, если знать о них хотя бы за несколько часов. В превентивном мониторинге используется принцип: «Предупрежден – значит, вооружен». Для целей информирования Центрального Банка России о возможных угрозах и их особенностях система мониторинга «ЛКС Аналитика» была настроена на сбор и систематизацию информации из российских и зарубежных сайтов: русскоязычных и англоязычных сайтов компьютерной тематики, сайтов правительств и министерств, форумов и объединений специалистов по информационной безопасности, сайтов компаний, разрабатывающих антивирусное программное обеспечение. В качестве оперативного варианта предоставления информации специалисты и руководители подразделений банка получают ежедневные сводки с важной информацией, которая систематизирована по типам угроз – вирусные угрозы, уязвимости, кражи денег с кредитных карт и т. д.

Мониторинг киберугроз решает несколько задач: предупреждает организацию о возможной угрозе безопасности, предоставляет техническим специалистам информацию об устройстве вирусов и особенностях проводимых хакерских атак, предоставляет информацию о технических новинках в антивирусном программном обеспечении и развитии средств защиты. Мониторинг компьютерных угроз – незаменимый элемент системы информационной безопасности, который позволяет оперативно отслеживать события в быстроменяющейся отрасли и постоянно развивать навыки специалистов по информационной безопасности.

Выводы. Благодаря гибкой настройке система мониторинга «ЛКС Аналитика» позволяет решать целый спектр задач в сфере безопасно-

сти. На сегодняшний день планируется установить ее на технической базе Московского университета МВД России имени В.Я. Кикотя, чтобы учащиеся университета получили доступ к современным технологиям мониторинга открытой информации.

Библиографический список

1. Сайт компании «Компьютерные системы ЛКС»: http://lksystems.ru.

2. Сайт компании «Лаборатория Касперского»: https://securelist.ru/ kaspersky-ddos-intelligence- report-for -q2-2016/ 28961.

3. Кукушкина О. В., Смирнов А. А., Соколов А. А. Текстология и «гипертекстология» Сети (редакционный обзор) // Портал http://www.textology.ru.

Д. Д. Савенкова[1]

ОТДЕЛЬНЫЕ НАПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ФИНАНСОВО-КРЕДИТНЫХ УЧРЕЖДЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

Проблема информационной безопасности в условиях развития глобального информационного общества приобрела особую актуальность. В связи с этим обращает внимание указание Президента Российской Федерации В. В. Путина Федеральному Собранию в Послании от 1 декабря 2016 г. на то, что в цифровых технологиях кроются риски и необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Это вопрос национальной безопасности и технологической независимости России, в полном смысле этого слова – нашего будущего» [1].

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, не только перечень угроз, а также совокупность средств, способных обеспечить надежную защиту информационной безопасности государства. Кроме того, также прямо указано, что общественные отношения в области обеспечения информационной безопасности как

[1] Менеджер департамента безопасности Сбербанка, Управление противодействия кибермошенничеству. © Савенкова Д. Д., 2018.

никогда нуждаются в правовом регулировании в связи с динамикой развития информационного общества, институализацией правовых институтов в области обеспечения информационной безопасности, являющейся важной составляющей национальной безопасности Российской Федерации. Жизнь множества людей незаметно для них самих во многом переходит в виртуальное пространство. И это явление, безусловно, ежедневно несет в себе все более новые угрозы. С увеличивающимся количеством пользователей сети «Интернет» растут и возможности у киберпреступников для совершения различного рода кибератак.

На сегодняшний день противодействие киберпреступности является проблемой мирового масштаба. Более того, киберпреступность превратилась в организованный бизнес, и достаточно прибыльный, в основе которого лежит, как правило, использование вредоносного программного обеспечения. Вредоносные компьютерные программы все чаще пишутся с целью незаконного обогащения за счет их дальнейшей перепродажи, а также в целях незаконного получения конфиденциальной информации пользователей и последующего хищения принадлежащих им денежных средств.

В России ежемесячная аудитория Интернета по состоянию на октябрь 2016 г. – март 2017 г. достигла 87 млн человек, что составляет 71% от всего населения страны [2]. По итогам 2017 г. число интернет-пользователей во всем мире впервые превысило 4 миллиарда человек, а современными мобильными устройствами (смартфонами) владеют около 2/3 населения планеты. На начало 2018 г. количество ежемесячных пользователей различных социальных сетей составило 3 миллиарда человек. При этом около 90% пользователей заходили на эти интернет-площадки через смартфоны [3].

Если говорить о финансово-кредитных учреждениях, можно сказать, что здесь наиболее распространено использование современных информационных технологий и сети Интернет, причем, как для удобства предоставления своим клиентам новых банковских продуктов и услуг, так и для быстроты осуществления денежных переводов, что не может не привлекать внимания злоумышленников.

За 2017 г. бизнес потерял примерно 116 млрд руб. из-за кибератак – убытки из-за киберпреступников признала почти каждая пятая российская компания [4]. Злоумышленники взламывали банкоматы, электронные кошельки и даже целые платежные системы. За последний год около 15 хакерских группировок атаковали государственные структуры, военные ведомства и частные компании [5]. По мнению аналитиков, ко-

личество киберпреступлений в России к 2018 г. грозит вырасти в четыре раза, а общие потери могут превысить 2 трлн руб. [6].

Для злоумышленников киберпреступления во многом привлекательны за счет того, что сегодня совершенно из любой точки земного шара злоумышленники могут осуществлять подготовку и совершение киберпреступлений, поскольку теряет в стоимости компьютерная техника, а объекты таких преступных посягательств не обязательно должны находиться в непосредственной близости от преступников. Характерно и то, что для совершения компьютерных преступлений не требуется прикладывать особые усилия и затраты, ведь достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. Глубокие технические познания также не обязательны – в сети «Интернет» можно найти большое количество специальных форумов, закрытых чатов в мессенджерах, в которых желающий может овладеть соответствующими познаниями и навыками, приобрести вредоносное программное обеспечение для последующего совершения правонарушений, похищенные номера кредитных карт, похищенные персональные и идентификационные данные пользователей, а также объединить усилия по проведению целенаправленных компьютерных атак на компьютерные системы различных объектов.

Открытость доступа к сети «Интернет» и, как следствие, затруднительность в отслеживании злоумышленников, позволяют им совершать большинство компьютерных преступлений с использованием именно данной сети. Анонимность всемирной сети «Интернет», уязвимость беспроводного доступа и использование прокси-серверов дают возможность существенно затруднить обнаружение злоумышленников – для совершения преступления может использоваться так называемая «цепочка серверов», о чем есть масса информации в открытом доступе в сети «Интернет», и этому навыку также можно научиться [7].

Как уже ранее было отмечено, компьютерные преступления (или киберпреступления) могут быть совершены абсолютно из любого местоположения, в частности, при помощи выхода в сеть «Интернет» через точки общего доступа (рестораны, кафе, общественный транспорт), ведь при помощи современных технологий возможно получить несанкционированный доступ к чужой беспроводной сети Wi-Fi. Более того, злоумышленнику не нужно выбирать место преступления исходя из местоположения потенциальной жертвы, что больше присуще классическим видам преступлениям – для использования своих технических средств при совершении компьютерных преступлений он может выбрать любое

удобное для себя место. Это еще одна отличительная черта, присущая компьютерным преступлениям – трансграничный характер.

Вышеперечисленные обстоятельства крайне затрудняют расследование компьютерных преступлений, которое требует максимально оперативного анализа и сохранения данных, которые ввиду своей уязвимости могут быть легко уничтожены злоумышленниками за считанные минуты.

По итогам 2017 г. наиболее распространенными преступлениями в сфере информационных и компьютерных технологий, с которыми пришлось столкнуться финансово-кредитным учреждениям, стали следующие:

– заражение вирусами рабочих компьютеров, в том числе с последующим вымогательством денежных средств;

– взлом почтовых ящиков сотрудников;

– атаки на сайты предприятий (взлом, вирусное заражение, DDoS-атаки);

– интернет-мошенничество или социальная инженерия (введение в заблуждение в целях получения денежных средств или конфиденциальной информации);

– несанкционированный доступ к информации предприятия;

– кража персональных данных клиентов;

– вмешательство в работу интернет-банкинга [7].

Вместе с тем, за аналогичный период времени Сбербанк называет основной угрозой кибербезопасности в банковской сфере не вирусы, а другой вид мошенничества – социальную инженерию (манипулирование поведением человека с использованием социальных и психологических навыков), на которую приходится 80 % всех атак на клиентов. Сбербанк ежедневно фиксирует около 2 тыс. обращений клиентов, связанных с мошенничеством, а за год в «черные списки» банка попадает около 50 тыс. мошенников, пытавшихся обмануть частных клиентов, и еще несколько тысяч, атаковавших юридических лиц [8]. Задачей любого злоумышленника, использующего методы социальной инженерии, является побуждение человека на доверии совершить необходимые от него преступнику действия, которые в нормальной жизни человек не стал бы делать.

Следует подчеркнуть, что чем стремительнее развивается сфера информационных технологий, тем больше новых видов киберпреступлений изобретают злоумышленники, которые не перестают совершенствовать свои навыки и придумывать новые способы незаконного обогащения в данной сфере. При этом государство также не должно отставать, а,

наоборот, наращивать темп проведения мероприятий, направленных на профилактику, предупреждение и борьбу с киберпреступностью, поскольку, как показывает правоприменительная практика, относительная длительность и бюрократический подход к развитию нормативно-правовой базы приводят к значительному отставанию таких мероприятий.

Как правило, успешные масштабные киберпреступления возможно совершать в рамках действия организованного преступного сообщества, членам которого не обязательно быть знакомыми лично, они могут знать друг друга лишь по никнеймам, используемым в сети «Интернет» при подготовке и совершении киберпреступлений. Одновременно с этим злоумышленники используют и традиционные методы совершения преступления, но, как правило, уже на его финальной стадии, а именно: при обналичивании похищенных денежных средств.

Таким образом, рост компьютерных преступлений именно в финансово-кредитной сфере требует от сотрудников правоохранительной системы помимо не только неукоснительного соблюдения и выполнения своих непосредственных служебных обязанностей по расследованию преступлений, но также понимания банковских процессов и финансовых отношений.

Обращает внимание проблема, связанная с нарушениями, допускаемыми сотрудниками правоохранительных органов при расследовании компьютерных преступлений. Органы прокуратуры отменяют каждое второе постановление об отказе в возбуждении уголовного дела по сообщениям о киберпреступлениях и о приостановлении расследования соответствующих уголовных дел [9]. Это происходит от того, что большая часть специалистов органов предварительного расследования занимается расследованием традиционных видов преступлений, либо они пытаются расследовать уголовные дела о киберпреступлениях традиционными методами, что абсолютно неэффективно. Необходимо помнить, что преступники всегда вооружены, быстро находят все более новые способы хищения денежных средств в сфере компьютерной информации, в то время как правоохранительным органам удается раскрыть незначительный процент от общего числа совершаемых киберпреступлений, учитывая суммы затрачиваемых государством бюджетных средств на содержание правоохранительных органов, что также неэффективно.

Есть и другая проблема в данном направлении, связанная с программой обучения следственных и оперативных работников правоохранительной системы. К примеру, курс криминалистики нуждается в кардинальном обновлении, поскольку он уже устарел. Радикально должны

быть переработаны и созданы новые курсы, изменены научные подходы к исследованию данных вопросов. Сбербанк осознает всю глобальность данной проблемы и первым в стране начал вести такую деятельность по направлению переподготовки специалистов, их обучение киберграмотности, информационной безопасности и основам банковской системы. Представляется, что тесное сотрудничество финансово-кредитных учреждений с правоохранительными органами, а также ведущими вузами страны в рамках вышеуказанных направлений позволит эффективнее вести борьбу с киберпреступностью [10].

Необходимо активное вовлечение и органов государственной власти в части, касающейся внедрения и разработки новых учебных программ на всех уровнях образовательной системы, что будет способствовать формированию правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности.

До недавнего времени судьи, прокуроры и следователи руководствовались в своей профессиональной деятельности нормативно-правовыми документами, которые уже устарели и не дают ответов на все актуальные вопросы, что мешает представителям названных ветвей власти не только иметь правильное представление о киберпреступлениях и механизмах их совершения, но и общий подход к толкованию и правоприменению.

Так, в одном из своих решений Московский городской суд оставил без удовлетворения апелляционное представление государственного обвинителя, которая просила отменить приговор суда первой инстанции, переквалифицировавшего действия виновного лица с ч. 2 и ч. 3 ст. 159 УК РФ на ст. 159.6 УК РФ.

Государственный обвинитель, мотивируя свою позицию, отметила, что «находит необоснованной и неправильной переквалификацию судом действий Д. со ст. 159 ч. 3 УК РФ по восьми преступлениям и ст. 159 ч. 2 УК РФ на ст. 159.6 ч. 2 УК РФ, указав, что для осуществления переводов денежных средств со счетов потерпевших Д. незаконно добился перевыпуска сим-карт потерпевших, используя которые путем введения достоверных логина и пароля осуществлял перечисление денежных средств потерпевших через систему «*** Онлайн». Данная судом квалификация этих действий как мошенничество в сфере компьютерной информации – несостоятельна, поскольку указанные действия образуют простое мошенничество» [11]. В ответ на это судебная коллегия апелляционной инстанции справедливо отметила, что, несмотря на то обстоятельство, что виновный Д. для входа в систему «*** Онлайн»

использовал подлинные логин и пароль при совершении преступления, оно не может служить основанием для совершения Д. простого мошенничества, не связанного с хранением компьютерной информации.

Таким образом, суд апелляционной инстанции квалифицировал действия виновного именно как вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Возражения прокурора судом были обоснованно отклонены.

На протяжении последних лет правоохранительные органы, принимая решения о квалификации действий виновного лица, также руководствовались некоторыми устаревшими положениями постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате». В частности, с появлением в 2012 г. шести новых специальных составов мошенничества некоторые положения вышеуказанного постановления Пленума фактически утратили актуальность.

В связи с этим, постановлением Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» признано утратившим силу Постановление № 51. Новое Постановление достаточно актуально как для сотрудников правоохранительных органов, так и для специалистов финансово-кредитных учреждений, поскольку даны разъяснения по многим актуальным вопросам. Во-первых, Верховный суд Российской Федерации обратил внимание на нормы закона, содержащиеся в Гражданском кодексе Российской Федерации, по смыслу которых, хищение чужого имущества охватывает собой понятие «электронные денежные средства». Таким образом, разъяснено, в каких случаях наступает уголовная ответственность за совершение хищения безналичных денежных средств, в том числе электронных денежных средств. Во-вторых, «социальная инженерия» должна квалифицироваться как кража (по ст. 158 УК РФ) [12]. Таким образом, в случае хищения безналичных денежных средств, когда злоумышленник получает к ним доступ, воспользовавшись той конфиденциальной информацией держателя платежной карты, которую он сам злоумышленнику сообщил под воздействием обмана, содеянное квалифицируется как кража. В-третьих, «фишинг» должен квалифицироваться как мошенничество (по ст. 159 УК РФ). Таким образом, в случае хищения чужого имущества или приобретения права на него, когда злоумышленник распространяет заведомо ложные сведения в сети «Интернет» (поддельные сайты, интернет-

магазины и т. д.), мошенничество квалифицируется по ст. 159, а не 159.6 УК РФ.

Кроме того, изменения, в которых, безусловно, нуждается российское законодательство в части противодействия киберпреступности, должно приниматься в соответствии с действующими международными нормативными правовыми актами (Будапештская Конвенция по киберпреступлениям от 23 ноября 2001 г., и др.), поскольку эффективное ведение борьбы с киберпреступностью, которая, как правило, носит международный характер, немыслимо на территории одного государства без международного сотрудничества.

Одним из ключевых направлений обеспечения информационной безопасности являются усиление государственно-частного партнерства и развитие соответствующих регионально-ориентированных программ с учетом экономической заинтересованности кредитных организаций в повышении уровня защищенности их информационных ресурсов. Представляется необходимым применение подходов, аналогичных тем, которые избраны в целях противодействия иным угрозам системного характера, например, таким, как коррупция [13].

Отдельно обращает внимание проблема недостаточного уровня киберграмотности населения. Большинство киберпреступлений совершается, в том числе, благодаря неосведомленности населения и клиентов кредитно-финансовых организаций, а также несоблюдения ими основных правил безопасности. В связи с этим значительную пользу в предупреждении киберпреступности имеют информационно-просветительские мероприятия в отношении новых рисков и угроз в информационных и компьютерных системах. Сбербанк регулярно предоставляет своим клиентам рекомендации по соблюдению кибергигиены, такие, например, как скачивание приложения «Сбербанк Онлайн» только с официальных ресурсов [14]. Данному направлению уделяет большое внимание и заместитель председателя правления Сбербанка С. К. Кузнецов, который справедливо отмечает важность соблюдения элементарных правил информационной безопасности, а именно: не пренебрегать антивирусом, создавать и использовать сложные пароли, не повторять их на всех используемых ресурсах, применять двухфакторную аутентификацию везде, где это возможно, использовать функции шифрования информации на жестких дисках, USB-носителях и применять шифрование для сохранения конфиденциальности переписки в Интернете [15].

Таким образом, можно сформулировать отдельные направления взаимодействия государственных органов и финансово-кредитных учреждений по противодействию киберпреступности в части обеспечения информационной безопасности:

1) содействие по созданию системы международной информационной безопасности, развитию сотрудничества с партнерами на глобальных и региональных площадках, таких как ООН, БРИКС, Шанхайская организация сотрудничества, АТЭС, ОДКБ, СНГ и других, проведению межведомственных консультаций и переговоров, что позволит более эффективно бороться с современными угрозами;

2) обоюдное сотрудничество в совокупности с усовершенствованием нормативно-правовой базы в области информационного законодательства Российской Федерации как основа правового фундамента для дальнейших практических шагов в направлении обеспечения информационной безопасности, предупреждения и пресечения компьютерных преступлений;

3) образовательные курсы для граждан в первую очередь для социально незащищенных категорий граждан и пожилых людей в целях повышения осведомленности старшего поколения о финансовом рынке, банках, их продуктах, современных технологиях и возможностях их применения, а также о том, как научиться распознавать мошенников, финансовые пирамиды, правила кибергигиены;

4) обучение слушателей учебных заведений и переподготовка следователей в целях обучения и формирования квалифицированных специалистов для органов внутренних дел, противостоящих преступлениям в сфере высоких технологий.

Библиографический список

1. Послание Президента Российской Федерации Федеральному Собранию от 01 декабря 2016 г.// СПС «КонсультантПлюс» (дата обращения: 01.02.2018).

2. Аудитория пользователей Интернета в России в 2017 г. составила 87 млн человек [Электронный ресурс] URL: http://2017.Russianinternetforum.ru/ news/ 1298.

3. В 2017 г. число интернет-пользователей впервые превысило 4 млрд. человек [Электронный ресурс]: http://oane.ws/2018/01/30/v-2017-godu-chislo-internet-polzovateley-vpervye-prevysilo-4-mlrd-chelovek. html.

4. Киберущерб превысил 100 млрд. Аналитики НАФИ подсчитали убытки бизнеса от хакерских атак [Электронный ресурс] URL: https:// www.rbc.ru/newspaper/2017/12/20/5a38f3749a79 4710 aa15581b.

5. Сбербанк объявил войну киберпреступности [Электронный ресурс] URL: http://vb.kg/economics/sberbank-obiavil-voiny-kiberprestypnosti.html.

6. К 2018 г. потери РФ от киберпреступлений превысят 2 трлн руб. [Электронный ресурс] URL: https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html.

7. Прокси в цепочке [Электронный ресурс] URL: https://xakep.ru/ 2001/08/24/13400.

8. Сбербанк назвал главную киберугрозу в банковской сфере [Электронный ресурс] URL: https://www.rbc.ru/rbcfreenews/ 5a27ef0b9a794 779 ffc 912e4.

9. Состоялось Координационное совещание руководителей правоохранительных органов по вопросам выявления и расследования преступлений в области информационно-коммуникационных технологий [Электронный ресурс] URL: https://genproc.gov.ru/smi /news/news-1122742.

10. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 134.

11. Апелляционное определение Московского городского суда от 06 мая 2013 г. № 10-2076// СПС «КонсультантПлюс» (дата обращения: 01.02.2018).

12. Русскевич Е. А. Разъяснения Пленума ВС РФ о квалификации мошенничества в сфере компьютерной информации // Уголовный процесс. – 2018. – № 2. – С. 33.

13. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 18.

14. Сбербанк посоветовал соблюдать «кибергигиену» из-за фальшивых приложений [Электронный ресурс] URL: https://www.rbc.ru/business/29/11/ 2017/5a1ed0c99a7947e8e144267b.

15. Кибергигиена – личное дело? [Электронный ресурс] URL: https:// iz.ru/news/670025.

С. В. Гурдин[1]

СОВЕРШЕНСТВОВАНИЕ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ТЕМЫ «ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Анализ современного этапа развития системы высшего образования в системе МВД Российской Федерации позволит утверждать, что оно направлено не только на повышение качества подготовки выпускников с учетом прикладного характера их будущей деятельности, но и на обучение их умелому и эффективному противостоянию совершенно новым угрозам национальной безопасности государства.

Одной из таких угроз является совершение преступлений в сфере компьютерной информации.

Так, на совместном совещании Генеральной прокуратуры Российской Федерации и Минкомсвязи по вопросам кибербезопасности и внедрению информационных технологий заместитель министра связи и массовых коммуникаций России Олег Пак сообщил, что количество киберпреступлений в России за три года выросло в шесть раз.

При этом рост киберпреступлений наблюдается не только в России, но и во всем мире, и это является следствием развития цифровой экономики.

Всемирная сеть стала неотъемлемой частью жизни многих людей, при этом многие пользователи Интернета даже не подозревают, какие опасности их поджидают во всемирной «паутине», и жертв киберпреступлений с каждым днем становится все больше и больше.

При таком положении дел особое значение приобретает качество подготовки и повышения квалификации лиц, осуществляющих предварительное расследование по уголовным делам о преступлениях в сфере компьютерной информации.

При этом следует учитывать тот факт, что действующее уголовно-процессуальное законодательство не предполагает, да и не может предполагать каких-либо особенностей в процедуре расследования таких преступлений.

Вместе с тем, его всесторонний анализ позволяет выделить некоторые особенности процесса доказывания по уголовным делам о пре-

---

[1] Доцент кафедры уголовного процесса МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Гурдин С. В., 2018.

ступлениях в сфере компьютерной информации. Соответственно лицу, осуществляющему доказывание по уголовным делам данной категории, необходимо обладать не только теоретическими знаниями особенностей этого вида деятельности, но и уметь грамотно и результативно применять их на практике.

Именно поэтому на кафедре уголовного процесса особое внимание уделяется преподаванию и совершенствованию методического обеспечения темы «Особенности доказывания по уголовным делам о преступлениях в сфере компьютерной информации». По сути, в качественной подготовке соответствующих специалистов в данном направлении, выражается вклад профессорско-преподавательского состава кафедры уголовного-процесса в совершенствование деятельности подразделений предварительного следствия органов внутренних дел по расследованию преступлений в сфере компьютерной информации в том числе совершаемых против собственности.

Учитывая небольшой объем преподавания темы в часах, нисколько не умоляя при этом значение методического обеспечения как процесса, остановлюсь более подробно на результате методического обеспечения темы, обеспеченного постоянной, планируемой, последовательной работы профессорско-преподавательского состава кафедры, который позволяет активизировать познавательную деятельность обучаемых и гарантированно достигать поставленные учебные цели вне зависимости от категории обучаемого контингента – будь то курсанты очной формы обучения или следователи, старшие следователи, специализирующиеся на расследовании преступлений в сфере компьютерной информации, которые повышают свою квалификацию.

В настоящее время методическое обеспечение темы представляет собой совокупность следующих методических документов, разработанных на кафедре или с участием профессорско-преподавательского состава кафедры:

1. Дополнительная профессиональная программа повышения квалификации «*Совершенствование деятельности подразделений предварительного следствия органов внутренних дел по расследованию преступлений в сфере компьютерной информации, совершаемых против собственности*», подготовленная авторским коллективом Московского университета МВД России имени В.Я. Кикотя.

2. Фондовая лекция по теме «*Особенности доказывания по делам о преступлениях в сфере компьютерной информации, совершаемых против собственности*», подготовленная в соответствии с указанной

выше Дополнительной профессиональной программой повышения квалификации следователей и отражающая такие особенности доказывания по этой категории уголовных дел, как:

– предмет доказывания, т. е. обстоятельства, подлежащие установлению по делам о преступлениях в сфере компьютерной информации;

– собирание, проверка и оценка доказательств по делам о преступлениях в сфере компьютерной информации;

– использование специальных знаний в области информационных технологий при производстве следственных действий;

– использование в доказывании по делам о преступлениях данной категории результатов оперативно-разыскной деятельности;

– получение информации по делам о преступлениях в сфере компьютерной информации, в рамках международного сотрудничества и использования ее в процессе доказывания.

В лекции на основе глубокого и всестороннего анализа действующего уголовно-процессуального законодательства, обобщения следственной и судебной практики даются достаточно четкие рекомендации относительно особенностей доказывания по уголовным делам о преступлениях в указанной сфере, приводятся конкретные примеры разрешения тех или иных вопросов, возникших в процессе доказывания на стадии предварительного расследования.

Кроме того, лекция позволяет получить обобщенные знания о современных путях решения проблемных вопросов доказывания, стоящих перед следователями, которые специализируются на расследовании преступлений в сфере компьютерной информации, в том числе совершаемых против собственности

3. *Методические рекомендации для проведения практических занятий,* содержание которых позволяет обучаемым не только упрочить знания, полученные при прослушивании лекции, но и выработать навыки принятия процессуальных решений в рамках специально воссозданных ситуаций, которые могут возникнуть в служебной деятельности лиц, расследующих уголовные дела о преступлениях в сфере компьютерной информации, в том числе совершенных и против собственности.

Такое становится возможным благодаря структурированной подаче материала обучаемым. Каждое занятие имеет теоретическую и собственно практическую составляющие.

Цель таких практических и лекционных занятий – углубленное изучение актуальных проблем теории и практики применения уголов-

но-процессуального законодательства, регламентирующего доказывание по данной категории уголовных дел, научных рекомендаций, приобретение новых умений и навыков в ходе практических занятий, необходимых для успешного выполнения должностных обязанностей следователей, старших следователей, специализирующихся на расследовании преступлений в сфере компьютерной информации, в том числе совершаемых против собственности.

4. Тестовые задания для проверки остаточных знаний по теме 4.3 «*Особенности доказывания по делам о преступлениях в сфере компьютерной информации, совершаемых против собственности*».

Выполнение тестовых заданий в процессе изучения темы является одной из форм контроля текущей успеваемости курсантов и слушателей Московского университета МВД России имени В.Я. Кикотя, а также следователей и старших следователей, проходящих повышение квалификации.

Тестовые задания состоят из контрольных вопросов, охватывающих объем изученного материала и практических заданий.

Тестовые задания содержат три возможных ответа, при этом только один из них является правильным. Предлагаемые тесты служат прежде всего реализации задач и достижению цели изучения темы 4.3, обеспечивая структурное восприятие материала, установление взаимосвязи в положениях отдельных вопросов. Решить тестовое задание обучаемые могут не только вспоминая пройденный материал, но и анализируя содержание предлагаемых вариантов ответов. Ответы на контрольные вопросы преследуют цель углубления полученных обучаемыми знаний и проверки уровня их подготовки, способности излагать и обосновывать свое мнение по поставленному теоретическому вопросу.

5. *Вопросы для комплексного экзамена*. В продолжение начатого разговора отметим что, несмотря то что все представленное выше методическое обеспечение достаточно актуальное, на кафедре осуществляется непрерывный процесс его совершенствования.

Активно обсуждаются на заседаниях предметно-методической секции и заседаниях кафедры новые, перспективные варианты наполнения методического обеспечения темы «Особенности доказывания по делам о преступлениях в сфере компьютерной информации».

Так, в разработке находится Практикум по указанной теме для курсантов очной формы обучения, который будет содержать в себе фабулу, набор процессуальных документов и другие необходимые атрибу-

ты, позволяющие обучаемым еще более полно усвоить полученные теоретические знания, развить в себе необходимые навыки принятия процессуальных решений и производства процессуальных действий, направленных на получение доказательств по уголовным делам о преступлениях в сфере компьютерной информации.

Рассматривается вопрос об использовании в процессе обучения *Деловой игры* по этой же теме, которая поможет обучаемым в формировании творческого типа мышления, инициативы, самостоятельности при принятии решений. Кроме того, по мнению участников предметно-методической секции и членов кафедры *Деловая игра*, способствует повышению знаний курсантов (слушателей) в области уголовно-процессуального законодательства, совершенствованию навыков анализа конкретной ситуации, связанной доказыванием по уголовным делам о преступлениях в сфере компьютерной информации, принятия процессуальных решений и их оформления.

Помимо этого профессорско-преподавательский состав кафедры, непосредственно осуществляющий преподавание указанной выше темы, постоянно повышает свою квалификацию посредством участия в различного рода семинарах, занятиях, проводимых сторонними организациями (Сбербанк России, Лаборатория Касперского и др.), круглых столах с участием представителей службы безопасности Сбербанка России, Лаборатории Касперского, следственных подразделений МВД России, на которых происходит обмен опытом и информацией, напрямую связанной с преподаваемой темой.

Изучаются реальные уголовные дела о преступлениях в сфере компьютерной информации, подвергаются всестороннему анализу судебные решения. Это позволяет обновлять практические ситуации, содержащиеся в методическом обеспечении темы и подлежащие разрешению обучаемыми, вносить новизну в приводимые примеры.

Таким образом, совершенствование методического обеспечения осуществляется на регулярной основе и представляет собой процесс улучшения качества комплекса средств дисциплины «Уголовный процесс» по уже известной, отдельно взятой теме для эффективного обучения курсантов очной формы обучения, а также повышения квалификации следователей и старших следователей, расследующих преступления в сфере компьютерной информации, в том числе и против собственности.

М. П. Суханова [1]

НЕОБХОДИМОСТЬ ВВЕДЕНИЯ ФАКУЛЬТАТИВА ПО КИБЕРБЕЗОПАСНОСТИ В НАЧАЛЬНОЙ И СРЕДНЕЙ ШКОЛЕ КАК ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ

Вопрос кибербезопасности в настоящее время является одним из важнейших для национальной безопасности России. Наше государство активно занимается проблемами противодействия киберпреступности в рамках программы по осуществлению важнейших принципов построения информационного общества. Это вызвано острой необходимостью появления общенациональной системы безопасности информационно-коммуникационной инфраструктуры, поддерживающих надежную ее защиту от различных угроз.

О киберпреступности опубликовано огромное количество разного рода публикаций и статей, что, безусловно, подтверждает, что для криминологического сообщества этот вид преступления является предметом особого внимания, но, несмотря на это, во всех подобных публикациях нет одного – сведений о реальном размахе киберпреступности, потому как получить подобные данные из общедоступных источников сбора эмпирической информации крайне затруднительно. Даже сотрудники специализированных оперативных подразделений правоохранительных органов не всегда располагают такими сведениями, т. к. особый механизм совершения киберпреступлений относит их к числу не просто высоколатентных, а сверхвысоколатентных.

Вместе с информационными и коммуникационными технологии, которые имеются в Интернете на данный момент и которые открывают невероятные возможности для всех возрастных категорий, к сожалению, все большую актуальность приобретает и проблема безопасности школьников в этом пространстве, отличающемся информационный многообразием и интенсивностью, множеством каналов влияний, вариативностью передаваемых ценностей, в связи с чем введение в начальной и средней школах факультативных занятий по кибербезопасности является одним из важнейших направлений в деле профилактики киберпреступности.

Имеющаяся на данный момент стратегия борьбы с киберпреступностью, в том числе с межгосударственными организованными ее

[1] Московский педагогический государственный университет. © Суханова М. П., 2018.

формами, включая киберпространство, за последние годы претерпела колоссальные изменения. Но на данный момент результаты этой стратегии по-прежнему не могут удовлетворить формирующееся в России информационное общество. Поиск оптимальных организационно-правовых форм противодействия киберпреступлениям ведется постоянно, в связи с тем, что киберпреступность постоянно видоизменяется, не представляется возможным использование статических или устоявшихся методов. МВД России стремится оперативно реагировать на развитие новых угроз кибербезопасности и вызовов национальной безопасности, принимая самое активное участие в противодействии киберпреступности [3].

В нашей стране в 2012 г. вступил в силу Закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [2]. По вышеуказанному Закону детям нельзя транслировать материалы, которые призывают к насилию (в отношении людей и животных) и самоубийству, курению, употреблению наркотиков и алкоголя, бродяжничеству, проституции. Также запрещено транслировать информацию, отрицающую традиционные семейные ценности, оправдывающую противоправное поведение, содержащую порнографию и нецензурную брань.

Законотворчество в области медиа трансформируется и совершенствуется, но несмотря на эти изменения, все еще остаются пробелы, наиболее явным из которых являются регулирование отношений в Интернете, а также доступ несовершеннолетних к этим ресурсам.

В связи с существенным и постоянно прогрессирующим числом пользователей среди детей и подростков проблема их безопасности в сети «Интернет» становится очень актуальной. При этом несовершеннолетние в гораздо меньшей степени, чем взрослые, готовы к проблемам, с которыми могут столкнуться в сети, и нередко остаются беззащитными перед ними. Дети и подростки на сегодняшний день наименее защищены от большого объема негативной информации в Интернете.

Даже при не очень активном поиске в Интернете легко попасть на сайты, где поощряются и оправдываются такие социально опасные явления, как сатанизм, сектантство, расовая и национальная нетерпимость, педофилия, различные виды сексуальных извращений, наркотики и т. п.

Кроме этого есть сайты, создаваемые организованным преступным группировкам и террористическим организациям, через которые они

не только обмениваются информацией, но и пытаются пропагандировать свои идеи и образ жизни. Школьники с неустоявшейся психикой при нахождении на такого рода сайтах могут воспринять пропагандируемые там взгляды и пробовать реализовать их в своей обычной жизни.

Сетевые технологии усиливают процесс опосредованного общения людей, участники которого чаще всего имеют поверхностные, неглубокие межличностные отношения. Возникающие здесь контакты чаще всего носят суррогатный характер. Иногда это приводит к сокращению влияния ближайшего окружения на личность подростка как средства социального контроля, нарушению механизмов детерминации позитивного поведения. Возможность анонимного участия в сетевом общении часто формирует у подростков представление о вседозволенности и безнаказанности любых проявлений в сетевой среде [1].

Чаще всего школьники оказываются на опасных страничках случайно. Всплывающие окна, неверно истолкованные поисковиком запросы, ссылки в социальных сетях – все это приводит ребенка на сайты небезопасного содержания, связанные с негативным контентом, киберхулиганством, виртуальными контактами с кибермошенниками, наркодилерами, экстремистами, педофилами. Значительное большинство подобных преступлений остаются скрытыми от родителей, правоохранительных органов и общества.

Пропаганда наркотиков, насилия и жестокости, суицидального поведения, самоповреждений весьма опасна для неустоявшейся детской психики. Ребенок верит во многие сомнительные идеи, особенно если они интересно для него изложены.

Для борьбы с опасным контентом Интернете путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей создаются разного рода общества.

Сегодняшние школьники часто с самого раннего возраста вовлечены в коммуникацию в виртуальном пространстве и не представляют себе мир без Интернета, где они находят возможности для получения новых знаний и общения.

Однако материалы, находящиеся в сети, не всегда можно однозначно расценить как способствующие развитию ребенка, становлению его как личности, а родители чаще всего не знают о способах защиты детей от подобного рода материалов.

Чтобы обеспечить информационную безопасность детей в Интернете и оградить их от неприемлемого контента, но при этом, не огра-

ничивая ребенка в доступности полезной информации, интернет-индустрия по всему миру пытается объединить усилия, направленные на обеспечение информационной безопасности детей.

Современные инновационные решения в этой области работают только в симбиозе с разумным регулированием государства, эффективным правоприменением и реализацией программ по обучению кибербезопасности всех пользователей в сети. Как одно из направление в этой программе может и должно стать введение в общеобразовательных школах факультативов по кибербезопасности, в результате работы которых дети будут иметь более расширенное представление о их правах и обязанностях, о последствиях их любых действий в сети, что обязательно будет служить одним из эффективных механизмов в деле профилактики киберпреступности.

Библиографический список

1. Андреев Б.В., Пристанская О.В. и др. Информационные технологии в расследовании преступлений, совершенных с использованием сотовой связи: научно-методическое пособие // Библиотека прокурора. – М. : Академия Генеральной прокуратуры Российской Федерации, 2009.

2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. от 01.05.2017 г.) // СПС «Консультант Плюс».

3. А. Мошков, начальник Бюро специальных технических мероприятий МВД России // URL: http://mvd.ru/news/item/830615/.

Ж. В. Кустарева [1]

МОДЕРНИЗАЦИЯ СИСТЕМЫ ОБРАЗОВАНИЯ В СВЯЗИ С РЕАЛИЗАЦИЕЙ ГОСУДАРСТВЕННОЙ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА»

Начало XXI в. символизирует ускорение развития цифровых технологий. Компьютеры и электронные системы, еще не так давно являвшиеся редкими участниками специализированных процессов, сегодня находят применение в любой сфере человеческой деятельности, часто весьма далекой от вычислительных направлений. Кроме того, именно посредством информационно-коммуникационных сетей сферы деятельности все теснее связываются между собой, постепенно образовывая определенное виртуальное пространство, знакомство с которым сейчас уже необходимо практически каждому человеку. В этих условиях представленная в июле 2017 г. Программа «Цифровая экономика Российской Федерации», разработанная в соответствии с поручением Президента России В. В. Путина [1], явилась своевременным решением глобализации цифровой экономики в России и интеграции ее с цифровыми экономиками зарубежных стран [2].

Понятие «Цифровая экономика» подразумевает систему экономических, социальных и культурных отношений, использующих цифровые информационно-коммуникационные технологии.

Цель Программы – развить и обеспечить следующие экономические, технические и социальные уровни:

1. Рынки и отрасли экономики, внутри которых осуществляется взаимодействие отдельных субъектов.

2. Платформы и технологии, в которых формируются компетенции для развития рынков и отраслей экономики.

3. Среда, создающая условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики и охватывающая нормативное регулирование; информационную инфраструктуру; образование и кадры; информационную безопасность [3].

Останавливаясь на сфере подготовки квалифицированных кадров и образования, следует подчеркнуть ее ключевое влияние на формирование человеческих ресурсов для обеспечения и развития Программы и поддержания ее конкурентоспособной при интеграции с мировыми

[1] Московский педагогический государственный университет. © Кустарева Ж. В., 2018.

цифровыми сферами. [4]. Для решения этой задачи в рамках Программы была создана рабочая группа, определившая следующие роли, функции и компетенции человека, отвечающего задачам Программы:

– адаптация к возможностям и ограничениям цифровой экономики;

– повседневное использование цифровых технологий;

– взаимодействие посредством цифровых ресурсов с разными отраслями жизни, в том числе властью, правовыми органами, СМИ, медиа;

– обладание компетенциями, обеспечивающими эффективную деятельность в условиях цифровой экономики: критическим и творческим мышлением, инициативностью, ответственностью, адаптивностью, инновационностью, предприимчивостью, эмоциональным интеллектом;

– понимание схемы функционирования и направлений эволюции цифровой экономики и наличие возможности участия в управлении ее конструкциями.

Развитие сферы подготовки кадров и образования не останавливается на образовательных программах, готовящих специалистов, уверенно действующих внутри цифровой экономики. Эволюцию должна претерпеть и документальная сторона сферы образования. Деятельность человека в цифровой экономике предполагает его обучение в течение всей жизни. Накопленные в цифровой среде данные о его учебной и профессиональной деятельности образуют его индивидуальную карьерную цифровую историю, на основе которой формируются цифровые документы, свидетельствующие о получении квалификаций и компетенций.

Таким образом, для соответствия системы образования и подготовки кадров требованиям цифровой экономики следует включить в эту систему следующие элементы:

– модель (описание) цифровых компетенций;

– цифровую среду, фиксирующую опыт и достижения участника цифровой экономики;

– систему проверки, аттестации и сертификации компетенций.

Среди направлений выполнения образовательной задачи Программы выделяются:

формирование образа выпускника, мотивация перспективных кадров;

– формирование образовательных стандартов, программ, систем оценивания, методов и способов образовательной деятельности;

– преемственность сфер образования (общего, дополнительного, профессионального);

– использование цифровых и сетевых технологий, сетевой информационной образовательной среды.

Помимо подготовки специалистов широкого круга, основным направлением также является подготовка участников бизнес-структур в цифровой сфере; специалистов по созданию, адаптации и внедрению технологий цифровой экономики; педагогов основного и дополнительного образования; специалистов по безопасности и защите информации в сети.

По мере развития предложения необходимо также развивать спрос, формируя рынок труда в направлении потребностей в специалистах цифровых технологий.

Таким образом, в сфере кадров и образования, согласно Программе, приоритетным являются:

– создание ключевых условий для подготовки кадров цифровой экономики;

– ориентирование системы образования на обеспечение цифровой экономики компетентными кадрами;

– развитие рынка труда, опирающегося на требования цифровой экономики;

– создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики в России.

Развитие информационной среды является не только целью, но и средством модернизации образования. Благодаря сетевой организации предоставления образовательных услуг стираются территориальные границы и сокращаются расстояния; появляется не только возможность, но и необходимость получать образование в любом возрасте и при любом уровне занятости; появляется возможность сообщения между специалистами, педагогами, участниками образовательной деятельности; возможность проведения открытых уроков, вебинаров, конференций; посещения электронных информационных ресурсов; оперативного и своевременного получения информации для повышения собственной квалификации [5].

Ориентируясь на современную действительность, необходимо выполнять планы по внедрению охватывающего все сферы жизни человека информационно-коммуникационного поля не только качествен-

но, но и быстро [6]. В рамках Программы в числе достижений, планируемых к сроку ее реализации, предусмотрены следующие достижения в области образования и кадров:

– увеличить количество выпускников учреждений высшего образования непосредственно по информационно-телекоммуникационным направлениям подготовки до 120 тыс. человек ежегодно (на сегодняшний день, согласно данным Программы, заявлено около 80 тысяч человек ежегодно);

– увеличить количество выпускников учреждений высшего и среднего профессионального образования, компетентных в IT-областях до 800 тыс. человек ежегодно (в сравнении с 300 тыс. человек ежегодно на сегодняшний день, согласно данным Программы);

– увеличить долю населения, обладающего цифровыми навыками, до 40 % от общей численности населения.

Библиографический список

1. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р//Справочно-правовая система «КонсультантПлюс».

2. Ход реализации программы «Цифровая экономика Российской Федерации». Портал Правительства России – http://government.ru/rugovclassifier/614/events/ .

3. Мохначев С. А. Развитие цифровой экономики и образование // Фотинские чтения. № 2 (8). – Ижевск: Частное образовательное учреждение высшего образования «Восточно-Европейский институт», 2017. – С. 7-10.

4. Шмелькова Л. В. Кадры для цифровой экономики: взгляд в будущее // Дополнительное профессиональное образование в стране и мире. № 8 (30). – Ярославль: ФГБОУ ДПО «Государственная академия промышленного менеджмента им. Н. П. Пастухова», 2016. – С. 1-4.

5. Чернышева Е. Н. Цифровая экономика и глобальное образование. // Актуальные проблемы контекстуального анализа ситуационно-регионального многообразия социального развития России в XXI в. – М. : Российский экономический университет им. Г. В. Плеханова, 2017. – С. 143-146.

6. Гончар В.В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 133.

Раздел 4. ПЕРСПЕКТИВНЫЕ МЕТОДЫ ИССЛЕДОВАНИЙ В ПРОТИВОДЕЙСТВИИ КИБЕРУГРОЗАМ

В. С. Власова[1]

ОСОБЕННОСТИ НАЗНАЧЕНИЯ СУДЕБНЫХ ЭКСПЕРТИЗ ПО УГОЛОВНЫМ ДЕЛАМ О МОБИЛЬНЫХ МОШЕННИЧЕСТВАХ

По рассматриваемой категории уголовных дел наиболее востребованы исследования электронных устройств, которые используются виновными лицами для хищений денежных средств со счетов банковских карт потерпевших: сотовые телефоны, планшетные компьютеры, ноутбуки, стационарные компьютеры.

Для исследования данных объектов назначается и проводится судебная компьютерная экспертиза [2], с помощью которой можно установить, закрепить и исследовать следы и признаки рассматриваемых преступлений, имеющиеся в памяти представленного на исследование устройства.

Помимо самих средств-носителей искомой информации (мобильный телефон, смартфон, персональный компьютер, ноутбук, планшетный компьютер, флеш-карты, жесткие диски, CD и DVD диски и пр.) в распоряжение эксперта целесообразно предоставить сведения, полученные от оператора связи (в рамках ст. 186.1 УПК РФ), подтверждающие (косвенно указывающие на) совершение определенных действий с мобильного устройства (смартфона, планшетного компьютера), направленные как на перевод денежных средств на счета третьих лиц, так и на завладение необходимой для этого информации – отправка соответствующих команд посредством SMS-сообщений, программ шпионов (Троянов, иного вредоносного ПО и пр.).

Примерными наиболее интересными для следствия вопросами, решаемыми в ходе производства рассматриваемой судебной экспертизы, могут быть:

1. Возможно ли осуществление доступа к сети «Интернет» с использованием представленных на исследование компьютерных средств (мобильного устройства)? Если да, то, каким образом осуществлялся доступ?

---

[1] Старший научный сотрудник первого отдела по исследованию криминалистических проблем Научно-исследовательского центра № 5 (по исследованию проблем расследования преступлений органами предварительного следствия и дознания) ФГКУ «ВНИИ МВД России». © Власова В. С., 2018.

2. Имеется ли на жестком магнитном диске системного блока персонального компьютера информация о том, что пользователь осуществлял работу на персональном компьютере в определенный период времени (указывается дата и время)? Если да, то когда (указать временные отметки) и с какими программами и файлами, периферийным оборудованием работал пользователь в указанный период времени? Подобные вопросы формулируются и по отношению к исследованию мобильного устройства, его внутренней памяти, внешних носителей информации (SD-карты).

3. Имеются ли признаки работы представленного компьютерного средства в сети «Интернет»? Каково содержание установок удаленного доступа и протоколов соединений?

4. Имеется ли в памяти мобильного устройства, представленного на исследование, информация об осуществлении сеансов доступа к сети «Интернет» за период с … по …, в том числе с использованием учетных данных …? Если да, то какие учетные данные использовались для выхода в сеть «Интернет»? В каких файлах содержатся сведения об использовавшихся логинах и паролях?

5. Имеются ли в памяти устройства признаки неправомерного доступа к данным (указывается интересуемый перечень конкретных признаков – программы «трояны», иное вредоносное ПО)?

6. Имеется в памяти мобильного устройства программное обеспечение, позволяющее без уведомления об этом пользователя, совершать какие-либо действия, передавать определенную информацию и пр.? Если да, то какое ПО, что оно позволяет, куда передает, и пр.?

7. Имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее сканировать ip-адреса компьютеров пользователей сети «Интернет», имеющих открытые для удаленного доступа из сети «Интернет» ресурсы? Если да, то такое программное обеспечение (название, версии, место расположения на носителе)? Имеются ли данные, свидетельствующие об использовании этого программного обеспечения? Если да, то какие именно?

8. Имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее подобрать пароль (захватить его при вводе)? Если да, то, какое программное обеспечение (название, версии, место расположения на носителе)?

9. Имеется ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее пользоваться услугами электронной почты? Если да, то, какое программное обеспечение (название, версии)? Имеются ли на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, информация о файлах, содержащих почтовые сообщения? Каков адрес электронного почтового ящика, на который получены входящие сообщения?

В целом на разрешение эксперта необходимо поставить ряд вопросов, позволяющих установить наличие в имеющихся электронных устройствах [1]:

– сохраненных текстов (SMS-сообщений) переписки между виновным и потерпевшим;

– истории посещения интернет-сайтов;

– наличие информации о поиске через установленный на устройстве браузер (Opera, Google Chrome, Internet Explorer, Safari и пр.) на Интернет сайтах сведений, имеющих отношение, например, к существующим вредоносным программам, позволяющим совершать хищения денежных средств со счетов и банковских карт, к способам распространения таких программ. Кроме того, могут быть обнаружены конкретные инструкции, носящие обучающий характер, в которых отражены последовательность и существо действий злоумышленников, заготовки диалогов, шаблоны SMS-сообщений, которые необходимо использовать при разговоре с потерпевшим (при SMS-общении), в целях провоцирования его к совершению действий, позволяющих завладеть принадлежащими ему денежными средствами;

– наличие установленных программ, предназначенных для мгновенной пересылки общений (например, ICQ (айсикью)), а также переписки (чатов) в этих программах;

– информации об использовании соответствующих Интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки);

– информации о регистрации в качестве пользователя в социальных сетях, на интернет-ресурсах (форумах), в том числе внутренних сетевых ресурсах интернет-провайдеров, на которых осуществляется обсуждение (обмен информации), демонстрация и распространение вредоносного ПО, обсуждаются вопросы его создания и пр.;

– информация, подтверждающая регистрацию виновного в качестве пользователя в локальной сети, организованной интернет-провайдером, в локальной папке пользователя которой также могут содержаться полезные для расследования сведения;

– сохраненных логинов и паролей (например, утилита операционной системы MacOs 10X «Связка ключей», при условии подтверждения пользователем сохранения пароля, содержит информацию о логинах и паролях всех когда либо посещенных сайтов);

– текстовых документов, фото-, аудио-, видеофайлов, прямо или косвенно указывающих на причастность пользователя устройства к использованию информации, сопряженной с рассматриваемыми преступлениями.

При назначении компьютерной экспертизы средств сотовой связи (мобильного телефона, смартфона, планшетного компьютера, оборудованного слотом для использования SIM-карты (модуль идентификации абонента)) необходимо, кроме вышеописанного, поставить перед экспертом комплекс вопросов, позволяющих: установить номер IMEI (международный идентификатор мобильного оборудования, состоящий из 15 цифр) телефона (смартфона, планшетного компьютера) в привязке к установленной SIM-карте в данном устройстве (при регистрации устройства в сотовой сети происходит привязка информации оператора связи, содержащаяся на SIM-карте к IMEI устройства, позволяющий идентифицировать владельца SIM-карты (абонента), по номеру IMEI устройства, и, наоборот, информация привязки «SIM-карта-IMEI» позволяет установить все IMEI номера устройств, работавших в паре с данной SIM), определить и скопировать всю содержащуюся в памяти устройства информацию (номера из абонентской книжки, SMS-сообщения, последние набранные номера, входящие вызовы, фото-, видео-файлы и пр.); определить и скопировать информацию из чатов, информация о которых содержится во внутренней памяти мобильного телефона и пр.

Данные и другие виды экспертиз по уголовным делам рассматриваемой категории рекомендуется назначать в государственных экспертных учреждениях системы МВД России и Минюста России, сотрудники которых имеют соответствующие допуски.

Библиографический список

1. Власов П. Е. Правовые основы производства контроля и записи телефонных и иных переговоров, как гарантии защиты прав участников уголовного процесса // Правовые и гуманитарные проблемы защи-

ты прав участников уголовного процесса : матер. междунар. науч.-практ. конф. – М. : МАЭП, 2008. С. 201–207.

2. Приказ МВД России от 29 июня 2005 г. № 511 (в ред. от 18.01.2017) «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации) // Российская газета. – 2005. – 30 авг.

В. И. Бокшицкий[1], И. С. Мельцева[2]

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ПРОИЗВОДНЫХ ПРИЗНАКОВ ОБЩЕСТВЕННОЙ ОПАСНОСТИ НЕЗАКОННОГО ОБРАЩЕНИЯ С КОНТРОЛИРУЕМЫМИ ТОВАРАМИ И ТЕХНОЛОГИЯМИ

Законодательство Российской Федерации в области государственного регулирования внешнеторговой деятельности и экспортного контроля основывается на Конституции Российской Федерации и состоит из Федеральных законов «Об основах государственного регулирования внешнеторговой деятельности» и «Об экспортном контроле», других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов Российской Федерации. Вопросы обеспечения экспортного контроля находятся в исключительном ведении Российской Федерации.

В соответствии со ст. 1 Федерального закона «Об экспортном контроле» контролируемыми товарами и технологиями признаются сырье, материалы, оборудование, научно-техническая информация, работы, услуги, результаты интеллектуальной деятельности (права на них), которые в силу своих особенностей и свойств могут внести существенный вклад в создание оружия массового поражения (ядерного, химического, биологического (бактериологического) и токсинного,

[1] Доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Бокшицкий В. И., 2018.

[2] Старший научный сотрудник учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Мельцева И. С., 2018.

средств его доставки (ракеты и беспилотные летательные аппараты), иных видов вооружения и военной техники, а также продукция, являющаяся особо опасной в части подготовки и (или) совершения террористических актов (технические устройства либо ядовитые, отравляющие, взрывчатые, радиоактивные или другие вещества, которые в случае их использования при подготовке и (или) совершении террористических актов создают реальную угрозу жизни или здоровью людей, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в том числе тяжких последствий, сопоставимых с последствиями применения оружия массового поражения). В соответствии со ст. 31 указанного федерального закона должностные лица организаций и граждане, виновные в нарушении законодательства Российской Федерации в области экспортного контроля, несут уголовную, административную и гражданско-правовую ответственность в соответствии с законодательством Российской Федерации.

В контексте настоящей работы значимыми охранительными нормами являются:

– в Уголовном кодексе Российской Федерации: ст. 189. Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники и статья 226^{1}. Контрабанда сильнодействующих, ядовитых, отравляющих, взрывчатых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных устройств, боеприпасов, оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а также материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов;

– в Кодексе Российской Федерации об административных правонарушениях: часть первая ст. 14.20. Нарушение законодательства об экспортном контроле.

Преступность и наказуемость незаконного экспорта из Российской Федерации или передачи контролируемых товаров и технологий закреплена нормами ст. 189 УК РФ. В соответствии с частью первой указанной статьи незаконный экспорт из Российской Федерации или

передача иностранной организации или ее представителю сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ для иностранной организации или ее представителя либо незаконное оказание услуг иностранной организации или ее представителю, которые заведомо для виновного могут быть использованы при создании вооружения и военной техники и в отношении которых установлен экспортный контроль (при отсутствии признаков преступлений, предусмотренных ст.ст. 226^1. Контрабанда и 275. Государственная измена УК РФ), наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок. Заведомое для виновного использование предмета преступления, как признак субъективной стороны преступления, выражает умышленный характер преступления [виновность в форме прямого или косвенного умысла], как обязательный признак субъективной стороны.

Таким образом, объективная сторона основного состава преступления, предусмотренного ст. 189 УК РФ, включает признаки незаконного экспорта или передачи в качестве предмета преступления контролируемых товаров и технологий, которые могут быть использованы при создании обычных видов вооружения и (или) военной техники. Указанное преступление относится в соответствии с частью второй ст. 15 УК РФ к категории преступлений небольшой тяжести.

Признаки особо квалифицированного состава преступления возникают, в соответствии с частью третьей ст. 189 УК РФ при изменении: а) субъектности преступления – при совершении его организованной группой; либо б) характера предмета преступления – при незаконном экспорте или передаче сырья, материалов, оборудования, технологий, научно-технической информации, работ (услуг), которые заведомо для виновного могут быть использованы при создании оружия массового поражения, средств его доставки и в отношении которых установлен экспортный контроль.

Принятые к настоящему времени Пленумом Верховного Суда Российской Федерации постановления о судебной практике и о вопросах, возникающих у судов при применении законодательства об уголовной ответственности в сфере предпринимательской и иной экономической

деятельности, законодательства об административных правонарушениях (КоАП РФ) и таможенного законодательства не содержат правил и рекомендаций по квалификации правонарушений в сфере экспортной деятельности (ст. 189 УК РФ и ст. 14.20 КоАП РФ).

Подробные рекомендации по квалификации преступления, предусмотренного ст. 226^1 УК РФ (в части контрабанды контролируемых товаров) содержатся в Постановлении Пленума Верховного Суда Российской Федерации от 27 мая 2008 г. «О судебной практике по делам о контрабанде». В связи с признанием указанного Постановления утратившим силу его следует рассматривать в качестве доктринального источника [48].

Результаты анализа судебных решений по делам, возбужденным по части третьей ст. 189 УК РФ и по части первой ст. 14.20 КоАП РФ, свидетельствуют о том, что в большинстве выявленных эпизодов предметом незаконного экспорта являлась химическая продукция, включенная в раздел 4 «Химикаты, которые имеют мирное назначение, но могут быть использованы при создании химического оружия», «Списка химикатов, оборудования и технологий, которые могут быть использованы при создании химического оружия и в отношении которых установлен экспортный контроль», утвержденного Указом Президента Российской Федерации от 28 августа 2001 г. № 1082. Материалов, переданных органами предварительного расследования на рассмотрение судов дел о незаконном экспорте иных видов контролируемых товаров и технологий (ядерных, химических и биологических), включенных в иные списки (перечни), выявлено не было.

Исследование материалов судебной практики по части третьей ст. 189 УК РФ и по части первой ст. 14.20 КоАП РФ показало, что фактические субъекты правонарушений являются во всех рассмотренных случаях специальными: лицами, выполняющими управленческие функции в коммерческих и иных организациях (по смыслу Примечания 1 к ст. 201 УК РФ), должностными лицами (по смыслу Примечания 1 к ст. 285 УК РФ и Примечания к ст. 2.4 КоАП РФ соответственно), а также для состава части первой ст. 14.20 КоАП РФ – юридическим лицами.

Основным фактическим признаком объективной стороны правонарушения, определяющим противоправный характер деяния, являлась передача контролируемых товаров нерезидентам или (и) их перемещение за пределы Российской Федерации в отсутствие у поставщиков необходимых экспортных лицензий ФСТЭК России.

Указанные обстоятельства объективно затрудняют с учетом содержания диспозиций частей первой – третьей ст. 189 УК РФ и части первой ст. 14.20 КоАП РФ в отсутствие соответствующих разъяснений Пленума Верховного Суда Российской Федерации процесс квалификации правонарушений в сфере экспортной деятельности как уголовных преступлений либо как административных правонарушений.

Незаконное переключение контролируемых товаров и технологий (в значении, полно выраженном ст. 1 Федерального закона «Об экспортном контроле» и конкретизированном нормами ст.ст. 189 и 226^1 УК РФ, частью первой ст. 14.20 КоАП РФ) является фактором высокой степени общественной опасности – источником и условием совершения тяжких и особо тяжких преступлений, прежде всего, террористического характера, направленных против публичных (национальных и международных) интересов, охраняемых уголовным правом Российской Федерации и зарубежных государств. Указанные общественно опасные деяния, направленные против мира и безопасности человечества, конституционного строя и безопасности любого государства, общественной безопасности, являются «универсальными» или «естественными» (mala in se – «преступления по их природе»), признаются преступными и наказуемыми во всяком цивилизованном обществе и всегда.

На основе результатов проведенного в рамках настоящей работы исследования автором предлагаются частные правовые категории: производное преступление и соответственно – производный состав преступления, совершаемого с использованием контролируемых товаров и (или) технологий. Термин «производный» выражает то обстоятельство, что необходимым условием совершения указанных преступлений является совершение первичных преступлений, включающих незаконное перемещение, передачу, присвоение контролируемых товаров и (или) технологий, посредством насилия, хищения, контрабанды, вымогательства, подкупа или дачи взятки либо иным незаконным способом. При классификации в отношении производных составов преступлений применена дополнительная группировка по следующим категориям:

1) обязательные производные составы преступлений, для которых в диспозиции норм уголовного закона включают обобщенные или детализированные указания на использование при совершении преступлений контролируемых товаров и (или) технологий;

2) факультативные производные составы преступлений с высокой вероятностью использования контролируемых товаров и (или) технологий, но без специального указания на данное обстоятельство в диспозиции уголовно-правовой нормы.

Библиографический список

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Российская газета. – 1993. – 25 декабря. – № 237.

2. Конвенция о физической защите ядерного материала. Совершено в городе Вене 26 октября 1979 г., открыто для подписания в городах Вене и Нью-Йорке 3 марта 1980 г. – URL http://nac.gov.ru/content/3906.html/. – дата обращения 08.01.2016.

3. Международная конвенция о борьбе с актами ядерного терроризма. Совершено в Нью-Йорке 14 сентября 2005 г., открыто для подписания в Центральных учреждениях Организации Объединенных Наций в городе Нью-Йорке 14 сентября 2005 г. – URL http://nac.gov.ru/content/3912.htm/ (дата обращения: 08.01.2016).

4. Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ // Собр. законодательства Рос. Федерации. – 1994. – № 32.

5. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собр. законодательства Рос. Федерации. – 1995. – № 33, ст. 3349.

6. Федеральный закон от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии» // Собр. законодательства Рос. Федерации. – 1995. – № 48, ст. 4552.

7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

8. Федеральный закон от 19 июля 1998 г. № 114-ФЗ «О военно-техническом сотрудничестве Российской Федерации с иностранными государствами» // Собр. законодательства Рос. Федерации. – 2003. – № 50, ст. 4850.

9. Федеральный закон от 18 июля 1999 г. № 183-ФЗ «Об экспортном контроле» // Собр. законодательства Рос. Федерации. – 1999. – № 30, ст. 3774.

10. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собр. законодательства Рос. Федерации. – 2001. – № 52 (ч. I), ст. 4921.

11. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 1, ст. 1.

12. Федеральный закон от 8 декабря 2003 г. № 164-ФЗ «Об основах государственного регулирования внешнеторговой деятельности» // Собр. законодательства Рос. Федерации. – 2003. – № 50, ст. 4850.

13. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Собр. законодательства Рос. Федерации. – 2011. – № 1, ст. 2.

14. Федеральный закон от 27 ноября 2011 г. № 311-ФЗ «О таможенном регулировании в Российской Федерации». – URL http://pravo.gov.ru/, дата обращения: 13.04.2017.

15. Указ Президента Российской Федерации от 28 августа 2001 г. № 1082 «Об утверждении Списка химикатов, оборудования и технологий, которые могут быть использованы при создании химического оружия и в отношении которых установлен экспортный контроль» // Собр. законодательства Рос. Федерации. – 2001. – № 36, ст. 3542.

16. Указ Президента Российской Федерации от 10 сентября 2005 г. № 1062 «Вопросы военно-технического сотрудничества Российской Федерации с иностранными государствами» // Собр. законодательства Рос. Федерации. – 2005. – № 38, ст. 3800.

17. Указ Президента Российской Федерации. 17 декабря 2011 г. № 1661 «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых установлен экспортный контроль» // Собр. законодательства Рос. Федерации. – 2011. – № 52, ст. 7563.

18. Стратегия национальной безопасности Российской Федерации. – Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 // Российская газета. – 2015. – 31 декабря.

19. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. – Интернет-портал Совета безопасности Российской Федерации URL http://www.scrf.gov.ru/documents/ (дата обращения: 30.12.2016).

20. Постановление Правительства Российской Федерации от 6 мая 2008 г. № 352 «Об утверждении Положения о системе государственного учета и контроля ядерных материалов» // Собр. законодательства Рос. Федерации. – 2008. – № 19, ст. 2188.

21. Справедливое судебное разбирательство в международном праве: юридический сборник. Опубликовано Бюро ОБСЕ по демократическим институтам и правам человека (БДИПЧ). – Ul. Miodowa 1000-251 WarsawPoland. – URL http://www.osce.org/odihr. 2013.

22. Бутков П. П. Терроризм и проблема безопасности в современном мире : учеб. пособие. – СПб. : СПбГУАП, 2004.

23. Журавель В. П. Актуальные проблемы предотвращения угрозы ядерного терроризма // Обозреватель – Observer. – 2011. – № 11. – С. 6–13.

24. Метельков А. Н. О некоторых аспектах уголовно-правового регулирования борьбы с проявлениями ядерного терроризма // Вестник МГТУ. – 2006. – № 1. – С. 157–162.

25. Паламарчук Е. А. Международный терроризм как глобальная проблема современности : учеб. пособие. – Ростов-на-Дону, 2010.

26. Совместная американо-российская оценка угрозы ядерного терроризма // Белферовский центр науки и международных отношений Института государственного управления им. Джона Ф. Кеннеди США, Массачусетс, Кембридж – Институт США и Канады Российской РАН.

27. Уголовное право. Общая часть. – М. : Изд-во Моск. ун-та, 1993.

28. Уголовное право. Общая часть : учебник. – 2-е изд, переработанное и дополненное / под ред. докт. юрид. наук, проф. Л. В. Иногамовой-Хегай; докт. юрид. наук, проф. А. И. Рарога; докт. юрид. наук, проф. А. И. Чучаева. – М., 2001.

29. Уголовное право России. Части Общая и Особенная : учебник / под ред. Н. Г. Кадникова. – М. : Юриспруденция, 2013.

30. Уголовное право Российской Федерации. Общая часть : учебник / под ред. проф. Б. В. Здравомыслова. – Изд. 2-е, перераб. и доп. – М., 2000.

31. Уголовно-процессуальное право : учебник / под ред. В. М. Лебедева. – М. : Юрайт-Издат, 2011.

32. Уголовно-процессуальное право Российской Федерации : учебник / отв. ред. П. А. Лупинская. – М., 2000.

33. Постановление Пленума Верховного Суда Российской Федерации от 10 октября 2003 г. № 5 «О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации». – URL http://www.vsrf.ru/ vscourt _detale.php?id=1177. – дата обращения: 11.12.2016. – Бюллетень Верховного Суда Российской Федерации. – декабрь. – № 12; Российская газета. – 2003. – 2 декабря 2003 г. № 244.

34. Постановление Пленума Верховного Суда Российской Федерации от 24 марта 2005 г. № 5 «О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях» (с изменениями, внесенными постановлениями Пленума от 25 мая 2006 г. № 12, от 11 ноября 2008 г. № 23, от 10 июня 2010 г. № 13, от 9 февраля 2012 г. № 3 и от 19 декабря 2013 г. № 40). – URL http://www.vsrf.ru/second.php, дата обращения 13.04.2017.

35. Постановление Пленума Верховного Суда Российской Федерации от 24 октября 2006 г. № 18 «О некоторых вопросах, возникающих у судов при применении Особенной части Кодекса Российской Федерации об административных правонарушениях» (с изменениями, внесенными постановлениями Пленума от 11 ноября 2008 г. № 23 и от 9 февраля 2012 г. № 2). – URL http://www.vsrf.ru/second.php, дата обращения 13.04.2017.

36. Постановление Пленума Верховного Суда Российской Федерации от 12 мая 2016 г. № 18 «О некоторых вопросах применения судами таможенного законодательства». – URL http://www.vsrf.ru/ second.php, дата обращения 13.04.2017.

37. Постановление Пленума Верховного Суда Российской Федерации от 15 ноября 2016 г. № 48 «О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности». – URL http://www.vsrf.ru/ second.php, дата обращения 13.04.2017.

38. Постановление Пленума Верховного Суда Российской Федерации от 27 мая 2008 г. № 6 «О судебной практике по делам о контрабанде» (с изменениями, внесенными постановлением Пленума от 28 сентября 2010 г. № 23) (признано утратившим силу – Постановление Пленума Верховного Суда Российской Федерации от 14 июля 2011 г. № 12). – URL http://www.vsrf.ru/second.php, дата обращения 13.04.2017.

39. Кассационное определение судебной коллегии по уголовным делам в составе председательствующего судьи В. Д. Шипиловой, судей Т. М. Шкурихиной, Н. И. Резановойот 15.02.2011 г. № 22-869 на приговор Неклиновского районного суда Ростовской области от 24.11.2010 г. / ч. 2 ст. 188 УК РФ, ч. 3 ст. 30, ч. 2 ст. 188 УК РФ, ч. 5 ст. 33, ч. 2 ст. 188 УК РФ, ч. 5 ст. 33, ч. 3 ст. 30, ч. 2 ст. 188 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com.

40. Апелляционное определение судебной коллегии по уголовным делам Северо-Кавказского окружного военного суда в составе: председательствующего судьи А. И. Каргина, судей С. М. Горелова и И. В. Костина от 07.07.2016 г. № 22А-323/2016 на приговор Крымского гарнизонного военного суда от 17.05.2016 г. / ч. 3 ст. 2261. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com.

41. Апелляционное определение судебной коллегии по уголовным делам Пермского краевого суда в составе председательствующего судьи А. В. Клюкина, судей Д. В. Отинова, Л. В. Гагариной, от 10 марта 2015 г. № 22-1314 на приговор Кировского районного суда г. Перми от 26.12.2014 / ч. 3 ст. 189 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

42. Саратовский районный суд Саратовской области, судья А. В. Беличенко, обвинительный приговор от 13.04.2016 г. № 1-71(1)/2016 / ч. 3 ст. 189 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https:// rospravosudie.com/, дата обращения: 13.03.2017.

43. Канавинский районный суд г.Нижнего Новгорода, обвинительный приговор от 25.02.2016 г. б/н / п. «а» ч. 2 ст. 2261 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

44. Октябрьский районный суд г. Екатеринбурга, судья Э. Р. Измайлов, Постановление о прекращении уголовного преследования и уголовного дела от 01.04.2015 г. б/н / ч. 3 ст. 189 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

45. Кировский районный суд г. Перми, судья Я. В. Литвинов, обвинительный приговор от 26.12.2014 г. № 1-391/14 / ч. 3 ст. 189 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

46. Суземский районный суд Брянской области, судья В. В. Клюев, обвинительный приговор от 25.02.2015 г. № 1-9-2015 / ч. 3 ст. 30 – ч. 1 ст. 2261; ч. 1 ст. 189 УК РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

47. Третьяковский районный суд Алтайского края, судья О. И. Каплунова, оправдательный приговор от 05.05.2015 г. № 3/2015 / ч. 1 ст. 2261 УК РФ, ч. 1 ст. 2261 УК РФ, ч. 1 ст. 2261 УК РФ, ч. 1 ст. 2261 УК РФ, с учетом ч. 1 ст. 14.20 КоАП РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com/, дата обращения: 13.03.2017.

48. Советский районный суд г. Нижнего Новгорода, судья Е. А. Синайко, постановление по делу об административном правонарушении, 2011 г. № 5-19/2011 / ч. ст. 14.20 КоАП РФ. – Материалы из банка данных ИС Росправосудие. – URL https://rospravosudie.com.

В. Г. Любан[1]

ОСОБЕННОСТИ РАБОТЫ БАНКОВСКИХ СЕРВИСОВ И ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ, ИСПОЛЬЗУЕМЫЕ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Направление борьбы с преступлениями в сфере информационных технологий (далее по тексту – ПИТ) в последнее время становится одним из приоритетных в деятельности органов внутренних дел. По этой причине следует обратить внимание на некоторые важные проблемные аспекты в этой сфере.

Раскрытие краж и мошенничеств в сфере информационных технологий в основной своей массе ложится на плечи подразделений уголовного розыска и на этом поприще им приходится испытывать большие трудности. По словам практических сотрудников из числа руководителей данных подразделений, латентность ПИТ чрезвычайно высока, а реальные цифры могут в несколько раз превышать официальную статистику.

Анализ способов совершения телефонных мошенничеств, SMS-фрода и мошенничеств на торговых интернет-площадках бесплатных объявлений позволил выявить ряд особенностей в работе банковских сервисов и в деятельности операторов сотовой связи, которые способствуют их совершению и активно используются преступниками.

Так, в сфере банковской деятельности можно выделить следующие проблемные аспекты.

Использование сервисов удаленной регистрации Интернет-банка. Как показывает анализ совершенных краж и мошенничеств, направленных на хищение средств с банковских платежных карт (далее по тексту – БПК) клиентов Сбербанка, большая доля этих преступлений связана с использованием сервисной услуги «Удаленная регистрация Сбербанк-онлайн». На различных интернет-форумах содержатся сотни гневных отзывов обманутых клиентов, которые свидетельствуют о применении к ним одного из способов, с задействованием данной сервисной услуги [1]. Несмотря на это, она продолжает функционировать до сих пор.

Механизм преступной схемы следующий:

---

[1] Доцент кафедры оперативно-разыскной деятельности и специальной техники МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Любан В. Г., 2018.

– злоумышленники в Интернете открывают официальную страницу сервиса «Удаленная регистрация Сбербанк-онлайн» [2] и вводят туда номер БПК, с которой предполагают похитить денежные средства;

– владельцу БПК на привязанный к ней телефон приходит цифровой пятизначный SMS-пароль, который преступники получают одним из трех способов: путем изготовления дубликата SIM-карты, путем заражения телефона компьютерным вирусом или с помощью социальной инженерии;

– преступники в течение двух минут осуществляют перерегистрацию Интернет-банка потерпевшего, установив новый логин и пароль;

– осуществив вход в Интернет-банк потерпевшего, преступники похищают его денежные средства, переводя их на подконтрольные себе БПК, банковские счета и балансы мобильных телефонных номеров.

Используя лазейку с удаленной регистрацией Интернет-банка, мошенникам не требуется иметь информацию о данных картхолдера, о сроке действия БПК, о CVV2 (CVC2) коде, о паспортных данных клиента, о кодовом слове, выбираемом в момент регистрации БПК и известном только банку и владельцу карты. Преступнику необходимо знать лишь номер БПК и номер привязанного к ней телефона. Причем эту связку «номер карты – номер телефона» они без труда могут найти в свободном доступе в Интернете на торговых площадках бесплатных объявлений, таких как «avito.ru», «irr.ru», «auto.ru», «am.ru» и других, где авторы объявлений часто сами выкладывают данную информацию для потенциальных клиентов.

Понятно, что сервис «Удаленная регистрация Сбербанк-онлайн» создавался в первую очередь для удобства клиентов и если раньше для регистрации личного кабинета в системе Сбербанк-онлайн приходилось идти в отделение банка или к ближайшему устройству самообслуживания, то теперь пройти регистрацию можно не выходя из дома всего за несколько минут. И в целом понятно желание Сбербанка идти в ногу со временем, не заставляя клиентов терять время, к тому же оно вполне оправдано для первичной регистрации клиентов в системе Сбербанк-онлайн, получивших БПК не в отделениях банка. Но главная проблема и основная претензия к этой услуге заключаются в том, что она позволяет проводить перерегистрацию уже зарегистрированных пользователей. В случае мошеннической атаки на телефон владельца БПК приходит всего одна SMS с паролем подтверждения, в которой не говорится о попытке перерегистрации Интернет-банка, поэтому уже зарегистрированный в нем человек может не осознать ха-

рактер мошеннических действий. Кроме того, SMS не содержит дополнительных предупреждений по поводу производимой перерегистрации, что упрощает преступникам задачу введения в заблуждение потенциальных жертв.

Справедливо возникает вопрос о целесообразности использования банками подобных сервисных интернет-услуг, которые не отвечают требованиям безопасности своих клиентов и активно используются преступниками.

Особенность работы автоматизированных систем самообслуживания клиентов через Интернет, позволяющих при входе в Интернет-банк (Мобильный банк). Эту особенность можно видеть на одной странице БПК, банковские счета и банковские вклады клиента и управлять ими.

Удобная в ряде случаев эта функция позволяет преступникам, преодолев систему безопасности только одной БПК потерпевшего и войдя в Интернет-банк, получить доступ ко всем его счетам и вкладам.

При этом «увести» деньги с вклада, на котором, как правило, имеется внушительная сумма, становится приоритетом для жуликов и не составляет им труда при наличии такового у потерпевшего. Для этого применяются методы социальной инженерии, и сначала «для отвода глаз» преступники зачисляют деньги на БПК самого потерпевшего. Потом мошенники перезванивают ему и под предлогом произошедшего сбоя системы просят вернуть поступившие клиенту деньги назад в банк, передав «оператору» приходящие на телефон пароли. Расчет у них на то, что, зачислив крупную сумму на БПК человека, он начнет недоумевать, станет верить в произошедший системный сбой и будет следовать инструкциям лжеоператоров банка. В целом назначение данной функции нам понятно, но малопонятно, зачем предоставлять клиенту доступ к долгосрочным вкладам через Интернет-банк (Мобильный банк), если клиент уже доверил их банку на длительный срок?

Возможность подключить (привязать) к одной банковской платежной карте несколько телефонных номеров для доступа к SMS-сервису «Мобильный банк», на все, из которых будут приходить SMS-сообщения с паролями подтверждения различных операций (в т.ч. транзакций). Подключить дополнительный телефонный номер клиент может разными способами: в отделении банка через операциониста, по телефону через сотрудника колл-центра, самостоятельно с банкомата или терминала самообслуживания. Например, к Мобильному банку одной БПК Сбербанк России сегодня позволяет «привязать» не

более восемь телефонных номеров, зарегистрированных в России (такое же количество БПК может быть «привязано» к одному телефонному номеру [3]). Однако подключаемый к Мобильному банку телефонный номер может быть оформлен не только на владельца БПК, а на совершенно любого человека (в том числе мошенника).

Преступники активно используют это обстоятельство, убеждая потерпевших под разными предлогами подойти к банкомату (терминалу) и ввести определенную комбинацию цифр, а иногда объясняют, что для успешного перевода средств необходимо сделать номер их телефона доверенным перед банком. Введенный таким образом в заблуждение человек сам подключает к Мобильному банку телефон мошенников, которые благодаря этому похищают денежные средства с БПК и вкладов потерпевшего. Как показывает практика, в подобных случаях банки не несут перед клиентом материальной ответственности за сохранность его финансовых средств по причине самостоятельно проведенных им операций.

Отсутствие строгих сроков хранения на банкоматах видеозаписей, которые сами по себе являются не только важной мерой профилактики возможных инцидентов (сдерживающим фактором), но и ценным источником оперативно-разыскной и криминалистической информации в процессе раскрытия и расследования преступлений. Например [6], для банкоматов Сбербанка России сегодня этот срок составляет от 0 до 60 дней. Другими словами, сохранность видеоинформации на этих банкоматах просто не гарантируется. Она может быть, а может и отсутствовать. При этом тенденция снижения техзащищенности банкоматов средствами видеофиксации повсеместно нарастает во всей банковской отрасли и связано это не только со сложностями хранения больших объемов информации, но и экономической нерентабельностью. Как известно из открытых источников, российские банки уже не первый год снижают расходы на охрану банкоматов. За первые 6 месяцев 2017 г. банки сократили эти затраты на 9%, а за АППГ этот показатель составил 8,6%. Со слов замначальника главного управления безопасности и защиты информации ЦБ России Артема Сычева, сегодня банки предпочитают страховать банкоматы, снижая расходы на охрану [4]. Данное обстоятельство играет на руку преступникам, затрудняет раскрытие и расследование ПИТ и на этом основании требует активного обсуждения со специалистами в банковской сфере.

В сфере деятельности операторов сотовой связи нами выделяются следующие проблемные аспекты:

1. Упрощенная процедура оформления и выдачи операторами сотовой связи дубликатов идентификационных модулей (SIM-карт).

В последнее время участились случаи совершения преступлений, сопровождающихся обходом технологии двухфакторной аутентификации (т.н. «3-D Secure») в целях установления контроля над Мобильным банком потерпевших, путем оформления дубликатов SIM-карт, привязанных к их БПК. Как правило, для этого мошенники используют «инсайдеров» – т. е. коррумпированных сотрудников салонов и офисов сотовой связи, а также поддельные доверенности. Очевидно, что органам внутренних дел вряд ли удастся повлиять на организацию работы сотовых компаний по отбору и проверке персонала, однако обязать сотовые компании оперативно предоставлять информацию банкам о совершенной замене SIM-карт кажется вполне реалистичной задачей. Это необходимо для того, чтобы банк, получив подобный сигнал, имел основания считать транзакции с этих номеров потенциально мошенническими и тщательней их перепроверял, а в случае необходимости мог и приостановить. Соблюсти при этом конституционные права граждан (на неприкосновенность частной жизни, личную и семейную тайну) и требования ФЗ № 152 «О персональных данных» не составит труда, если операторы сотовой связи будут представлять банкам обезличенные персональные данные, например, только информацию о дате состоявшейся замены, причине замены и телефонном номере абонента. В качестве дополнительной профилактической меры можно предложить банкам ввести запрет на проведение операций через Интернет-банк и Мобильный банк в течение нескольких суток после замены SIM-карты, а в случае такой необходимости, рекомендовать клиентам обращаться в отделение банка.

2. Предусмотренная операторами сотовой связи возможность зачисления крупных сумм денежных средств на баланс номеров мобильных телефонов.

Известны случаи, когда преступники, используя данное обстоятельство, с помощью банковского трояна или социальной инженерии получали контроль над Мобильным банком потерпевшего и переводили сотни тысяч рублей с его БПК на балансы разных телефонных номеров, оформленных на подставных лиц. Для дальнейшего выведения денег преступники используют услуги сотовых операторов по переводу средств с баланса телефонного номера на БПК, на банковский счет или на другой телефон. Подобные услуги сегодня есть в арсенале всех сотовых операторов и называются «Мобильные платежи» (Мегафон),

«Денежные переводы» (МТС), «Мобильный перевод» (Билайн) и т. д. Надо сказать, некоторые ограничения на перевод денежных средств у сотовых операторов все же имеются. Например, в МТС возможны разовые платежи до 15 тыс. руб., а в сутки допускается не более пяти платежей. В Мегафоне ограничение на все переводы (на телефон, на счет, на карту) сейчас составляет 40 тыс. руб. в месяц, которые можно совершить и за один день. Однако имеющиеся ограничения на суммы переводов не создают препятствий преступникам и вместо того, чтобы сразу перевести всю сумму на какой-то номер, они переводят ее частями на разные телефонные номера.

Таким образом, сегодня наблюдаются признаки перехода сотовых операторов в сферу банковских услуг, так как они выпускают свои БПК, выдают микрозаймы, а сам телефонный абонентский номер стал нечто средним между БПК и банковским счетом, ограниченными по объему зачисляемых средств и по функционалу представляемых услуг. Телефонный номер абонента привязан к определенному внутреннему финансовому лицевому счету, на нем можно держать деньги, с него можно оплачивать услуги, на него можно получать денежные переводы и с него можно отправлять переводы. В связи с тем, что данные инструменты используются для легализации (отмывания) денежных средств, полагаем, сотовые операторы должны ограничить разумной суммой размер средств на счетах мобильных номеров, достаточной только для оплаты услуг связи, а банковские услуги оставить банкам.

3. Заинтересованность операторов сотовой связи в распространении анонимных идентификационных модулей (SIM-карт).

Можно констатировать отсутствие до сих пор адекватной законодательной и общественной реакции на данный факт несмотря на то, что за последнее время в целях борьбы с анонимностью в Интернете был принят целый ряд законов. Но ситуация такова, что ужесточение санкций и введение самых строгих правил в отношении абонентов сотовой связи и пользователей Интернета окажется безрезультатным в условиях, когда на улицах бесплатно раздаются анонимные SIM-карты, являющиеся, как было указано выше, по сути, банковским платежным инструментом. Используя такую SIM-карту, злоумышленники с минимальным для себя риском могут отправить сотни SMS-сообщений или электронных писем с угрозой терактов, вложенными вредоносными компьютерными программами, криминальным спамом или просто осуществить звонки, преследуя мошеннические цели. По всей видимости, сегодня это мало беспокоит операторов связи, но

должно беспокоить органы внутренних дел, которым еще предстоит выяснить, как SIM-карты, которые должны распространяться через дилерские сети, офисы и салоны связи, проходя оформление перед регистрацией в сети, тысячами оказываются на улице в руках у случайных людей и, как следствие, у криминала.

Очевидно, что находящийся с 22 мая 2017 г. на рассмотрении в Государственной Думе законопроект № 181342-7, предполагающий введение административной ответственности за распространение неуполномоченными лицами идентификационных модулей, давно перезрел и даже в случае его принятия уже вряд ли достигнет ожидаемого эффекта [5]. По нашему мнению, законодатель должен обязать операторов сотовой связи распространять идентификационные модули только в салонах и офисах связи, заставив их отказаться от порочной практики реализации SIM-карт через третьих лиц. Аналогичного подхода необходимо придерживаться в вопросах государственного регулирования обращения БПК, распространять которые следует только через банковские учреждения, так как сегодня широко распространилась практика оформления и выдачи БПК в магазинах, АЗС, салонах сотовой связи и других местах.

Злоумышленники владеют информацией о перечисленных обстоятельствах и используют их в своих преступных планах. Поэтому в целях противодействия преступлениям в сфере информационных технологий, рассмотренные особенности в работе банковских сервисов и в деятельности операторов сотовой связи требуют широкого обсуждения со специалистами.

Библиографический список

1. URL: https://forums.drom.ru/garazh/t1152249437.html.
2. URL: http:// irecommend.ru/content/ostorozhno-moshenniki-moi-otzyv-o-tom-kak-ya-chut-ne-stala-zhertvoi-moshennichestva-i-chto-t и др.
3. URL: https://online.sberbank.ru/CSAFront/async/page/registration.do.
4. URL: http://banki-v.ru/karty/kak-privyazat-kartu-sberbanka-k-telefonu/.
5. URL: http://www.vestifinance.ru/articles/92172.
6. Законопроект №181342-7 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях (в части установления административной ответственности за распространение неуполномоченным лицом идентификационных модулей, а также за непредставление или несвоевременное представление оператору связи сведений, предусмотренных правилами оказания услуг связи)» (URL: http://asozd2. duma.gov.ru/ main.nsf/(Spravka)?OpenAgent&RN=181342-7).

Е. Л. Евраев[1], Д. Н. Захаров[2]

МЕТОДИКА ИССЛЕДОВАНИЯ ОБРАЗОВ НЖМД С ЦЕЛЬЮ ПОИСКА СЛЕДОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

Глубокая компьютеризация инфраструктуры в развитых странах непосредственно привела к бурному развитию технических средств разведки (ТСР), которые позволяют находить конфиденциальную или секретную информацию из компьютеров и компьютерных сетей.

Перспективность данного направления непосредственно обусловлена неуклонно растущим документооборотом, который осуществляется с помощью электронных средств, и внедрением «безбумажных технологий» как в сфере бизнеса, так и в сфере государственного управления.

Значительные объемы секретных данных, которые непосредственно хранятся в базах данных ПК различных правительственных и неправительственных структурах, представляют собой реальную коммерческую значимость, а их утечка в ряде случаев способна оказывать влияние на безопасность государства.

В особенности уязвимыми оказались так называемые «открытые» сети, имеющие выход в Internet, и регулярно подвергающиеся атакам хакеров и маскирующихся под хакеров спецслужб различного уровня.

В основной массе вычислительных систем (ВС) органов государственной власти в качестве основного энергонезависимого носителя данных используется накопитель на жестком магнитном диске (НЖМД). Об этом свидетельствует постоянно растущий поток публикаций, посвященных разработке всевозможных систем шифрования, разграничения доступа, закрытия электромагнитных каналов утечки и т. д.

В большинстве вычислительных систем (ВС) органов государственной власти в качестве основного энергонезависимого носителя информации используется накопитель на жестком магнитном диске (НЖМД).

---

[1] Слушатель 517 учебного взвода 5 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Евраев Е. Л., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Захаров Д. Н., 2018.

HDD (Hard Disk Drive – устройство управления жесткими дисками, винчестер, жесткий диск, дисковод жестких дисков, накопитель на жестком магнитном диске (НМЖД), Hard Magmetic Disk Drive (HMDD)) используется для хранения больших объемов информации пользователя.

Строение и принцип работы НЖМД. Жесткий диск помещен в герметичную железную коробку, в которой размещены магнитные диски, блок головок для чтения и записи и электродвигатель.

При включении ПК электродвигатель раскручивает магнитный диск до скорости в несколько тысяч об/мин, и диск вращается в течение всего времени, пока ПК включен.

Вследствие высокой скорости вращения диска специальные магнитные головки, которые записывают и считывают информацию, «парят» над ним. При касании головок к диску он быстро пришел бы в негодность.

Угрозы данных, хранимой на НЖМД. В настоящее время большинство государственных организаций и обычных пользователей пришли к пониманию значения задачи защиты данных и внедряют технические средства, позволяющие обеспечить безопасность на различных этапах жизненного цикла данных – при вводе, обработке, пе-

редаче и хранении. Однако последнему этапу – утилизации данных – часто уделяется недостаточно внимания.

К особенностям жесткого диска, делающим его привлекательным для проведения мероприятий с использованием ТСР, следует отнести:

– большие объемы хранимых данных, от сотен Мбайт до десятков Гбайт;

– энергонезависимость хранимых данных, так как на ее состояние не влияет наличие либо отсутствие электропитания;

– отсутствие в России собственного производства НЖМД.

Контроль охватываемого НЖМД стандартными орудиями диагностики неосуществим, так как для них он неработоспособен.

Стереть данные с «неисправного» накопителя невозможно по той же причине.

Исходя из практики крупных отечественных компаний, заключающих договора на создание и обслуживание компьютерных сетей с не менее крупными зарубежными корпорациями, так, как правило, и происходит.

Цифровой след (артефакт) – любая компьютерная информация, способная помочь следствию.

Виртуальные следы – это следы совершения действий в информационном пространстве технических устройств, их сетей и систем, такие как: создание, включение, удаление, внесение изменений, активация, открывание. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами [1].

Места поиска цифровых следов. Базы программ обмена сообщениями: Формат базы сообщений sqlite; SQLite Manager; Базы почтовых программ(MS Outlook) (когда пользователь мессенджера удаляет сообщения, SQLite не уничтожает их, а отмечает как удаленные…).

Объекты хранения информации: Personal Address Book (PAB), которая содержит контакты (файл имеет расширение .pab); Personal Storage Table (PST) – содержит e-mails, события календаря, задачи, заметки и др. (файл имеет расширение .pst); Offline Storage Table (OST) – содержимое как в PST, но может быть использовано в MS Exchange; системные журналы событий.

Журнал событий – стандартный способ для приложений и операционной системы записи и централизованного хранения информации о важных программных и аппаратных событиях.

Доступ к журналам событий:

– в ОС Windows (консоль просмотр событий – Пуск-Панель управления – Администрирование – Просмотр событий);

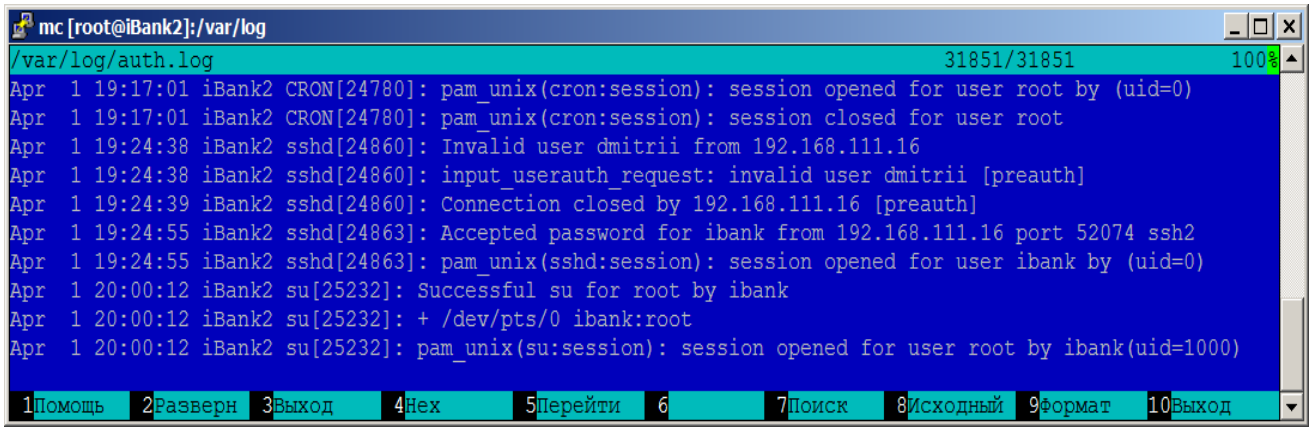
–в Mac OS X (располагается в виде файлов в каталоге /var/log; имеет графическую утилиту для просмотра Программы-Утилиты-Консоль; лог-файлы в Mac OS X – каталог /var/log основного системного журнала system.log; install.log);

– в Linux (расположены в каталоге /var/log: сгруппированы по службам).

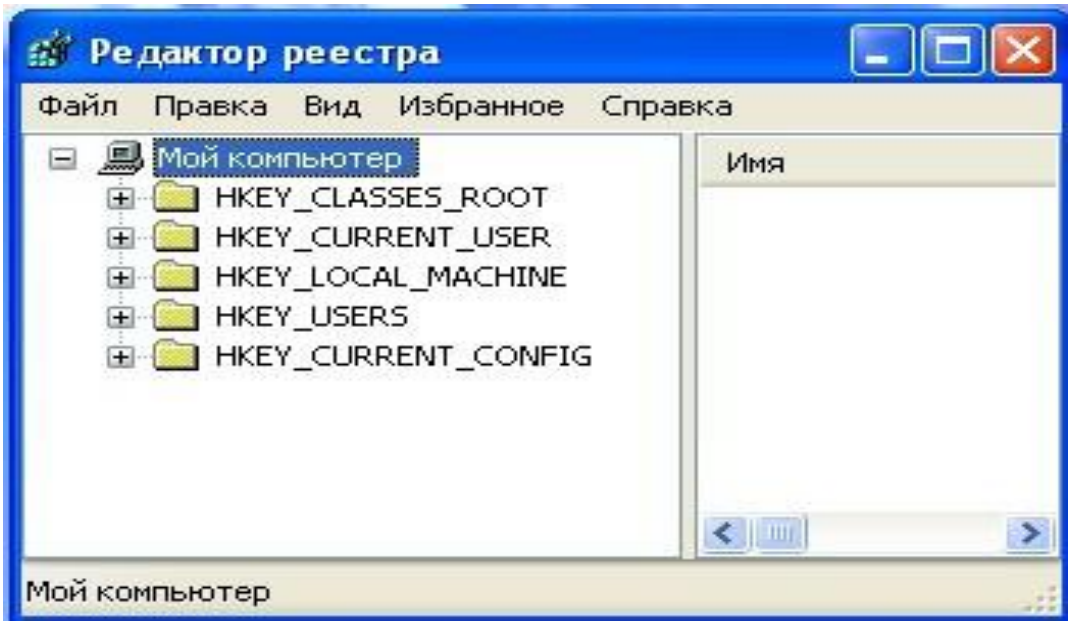
Важны для анализа и конфигурационные файлы ОС Unix (хранятся в каталоге /etc – /etc/HOSTNAME – /etc/passwd – /etc/profile – /etc/sudoers – /etc/crontab – /var/log/auth.log).

Не забываем анализировать и регистрацию попыток входа, и регистрацию IP-адреса входа, а также типа аутентификации.

На рисунке приведена попытка повышения привилегий:



Реестр ОС Windows. Реестр Windows – иерархически построенная база данных параметров и настроек.



Реестр содержит информацию и настройки для аппаратного обеспечения, программного обеспечения, профилей пользователей, предустановки.

Большинство изменений в Панели управления, ассоциации файлов, системные политики, список установленного ПО фиксируются в реестре.

Используемый софт: Autopsy (Autopsy Forensic Browser) – удобный веб-интерфейс (WebUI) к набору консольных утилит, предназначенных для проведения криминалистического анализа файловых систем The Sleuth Kit (TSK).

```
NAME
       autopsy - Autopsy Forensic Browser

SYNOPSIS
       autopsy  [-c]  [-C]  [-d  evid_locker ] [-i device filesystem mnt ] [-p
       port ] [addr]

DESCRIPTION
       By default, autopsy starts the Autopsy Forensic Browser server on  port
       9999  and  and  accepts  connections from the localhost.  If -p port is
       given, then the server opens on that port and if addr  is  given,  then
       connections  are only accepted from that host.  When the -i argument is
       given, then autopsy goes into live analysis mode.

       The arguments are as follows:

       -c     Force the program to use cookies even for localhost.

       -C     Force the program to not use cookies even for remote hosts.

       -d evid_locker
              Directory where cases and hosts are stored.  This overrides  the
              LOCKDIR  value  in  conf.pl.  The path must be a full path (i.e.
              start with /).
```

The Sleuth Kit (TSK) – набор автоматизированных инструментов для проведения криминалистического анализа файловых систем. В состав набора входят библиотека и более двадцати консольных утилит, большинство из них для удобства пользователя разбиты на группы, каждая из утилит набора является низкоуровневой и выполняет одну простую задачу [2].

Autopsy поддерживает несколько режимов анализа (соответствующих структуре пакета TSK), в режиме анализа файлов можно просматривать списки файлов и каталогов, а также содержимое отдельных файлов. Анализ в режиме метаданных отображают все метаданные связанные с конкретной записью и всех блоков данных. Режим блоков данных позволяет просмотреть содержимое любого блока данных файловой системы (как в шестнадцатеричном редакторе), в режиме поиска по ключевым словам возможен поиск по ASCII-кодам и

строкам Unicode (поиск осуществляется по логическим томам, а не по логическим файлам).

Из вышесказанного можно сформировать заключение, то что безопасное ликвидирование секретной информации с энергонезависимых носителей является значимой проблемой, в отсутствии постановления каковой нереально формирование безграничной системы защиты сведений в автоматизированных информационных системах организаций общегосударственной власти.

Цифровой отпечаток – это любая криминалистически важная компьютерная информация, т. е. данные (уведомления, сведения), пребывающие в электронно-цифровой форме, отмеченные в физическом носителе с поддержкой электромагнитных взаимодействий или переходящие согласно каналам связи с помощью электромагнитных сигналов.

Цифровые отпечатки считаются вещественными незаметными отпечатками. В базе механизма их создания возлежат электромагнитные взаимодействия двух и более материальных предметов – справедливых форм существования компьютерной информации.

Воздействие одной объективной формы жизни компьютерных сведений в иную (связь предметов следообразования) способно быть найденным согласно наблюдаемому отличию среди трех популярных их состояний.

Библиографический список

1. Бахорев А. А., Иванов В. Ю. Возможности получения информации с поврежденных жестких магнитных дисков // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : 2016. С. 102–105.

2. Слюнкина А. Д., Иванов В. Ю. Исследование короткоживущих данных при расследовании компьютерных преступлений // В сборнике: Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 62–65.

Ю. А. Павенский[1], *В. Ю. Иванов*[2]

МЕТОДЫ ИССЛЕДОВАНИЯ ДАМПОВ ОПЕРАТИВНОЙ ПАМЯТИ В ЦЕЛЯХ ОБНАРУЖЕНИЯ СЛЕДОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Экспертная задача: исследование информации, хранящейся в файлах.

В данном случае будет устанавливаться только та информация, которая присутствовала в ОЗУ на момент снятия дампа. К такой информации можно отнести: список выполняющихся процессов; ветви реестра, которые были задействованы при работе в операционной среде; список процессов, производящих обмен пакетами как в сети «Интернет», так и в локальной сети (LAN), с указанием подробных сведений о данных пакетах; инструкции программ, которые были оставлены в памяти после их выполнения; изображения, которые просматривались пользователем операционной среды и т. д.

В зависимости от требуемой информации техника исследования может быть: автоматизированной, ручной и комплексной.

Оборудование:

Виртуальная машина (рекомендуется использовать VMware Player или Oracle VM VirtualBox).

Операционная среда. При использовании автоматизированного метода – Sift Workstation 3.0, а при использовании ручного – на усмотрение эксперта.

Специальное программное обеспечение, предназначенное для отладки (дизассемблирования) программ и HEX-редактор (при использовании ручного метода).

Итак, в качестве примера рассмотрим два основных метода:

Метод проведения исследования, основанный на использовании стандартных средств операционной системы «Sift Workstation 3.0». В ходе проведения исследования были использованы: дамп оперативной памяти (файл ram.vmem); виртуальная машина VMware Player версии 6.0.3; операционная система Sift Workstation 3.0.

---

[1] Слушатель 518 учебного взвода факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Павенский Ю. А., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Иванов В. Ю., 2018.

Выполним команду vol.py -f /home/sansforensics/Desktop/ram.vmem imageinfo для определения профиля, под которым будем исследовать дамп оперативной памяти. Допустим, мы определили профиль Win7SP1x64, теперь вводим команду vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 pstree для просмотра выполняющихся процессов в оперативной памяти и обнаружим, например, троянский процесс mimi.exe и какой-то подозрительный процесс под названием 5:2878BK, который не имеет расширение *.exe (см. рис. 1) [2, 3].

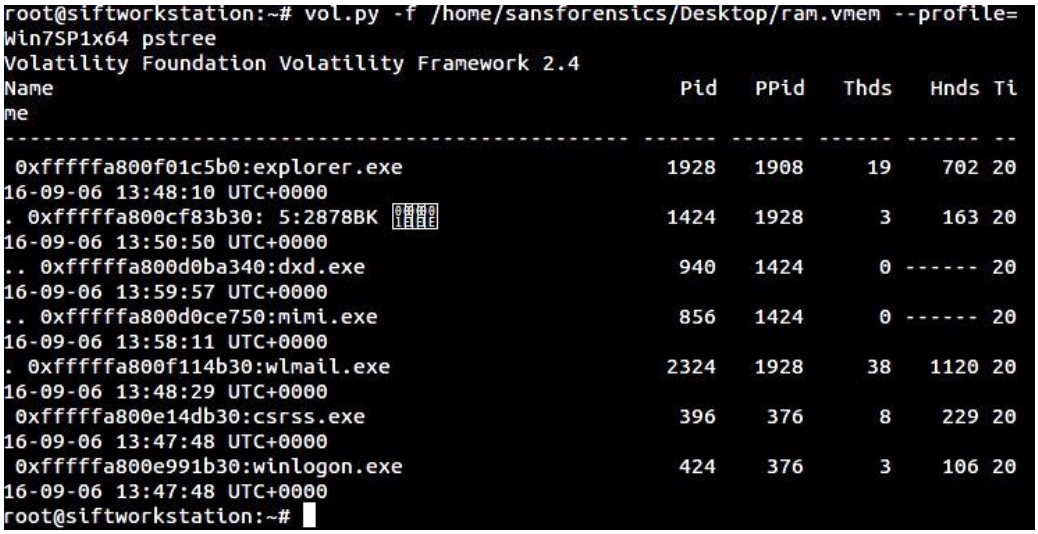


Рис. 1. Обнаружение выполняющихся троянских процессов

Теперь посмотрим на сетевую активность выполняющихся процессов в оперативной памяти, введя команду:

vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win 7SP1x64 netscan и увидим подозрительную сетевую активность со стороны процесса, расположенного по смещению: 0x3dbec910 TCPv4 192.168.180.131:49212 192.168.1.100:8080 ESTABLISHED 1424 5:2878BK.

Это говорит о том, что на момент снятия дампа оперативной памяти данный процесс осуществлял передачу сетевых пакетов с интерфейса 192.168.180.131:49212 на интерфейс 192.168.1.100:8080 (см. рис. 2).

Для исследования реестра необходимо ввести команду (рис. 3):

vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 hivelist.

```
root@siftworkstation:~# vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.4
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0x3dd5c690         UDPv4    0.0.0.0:3702                   *:*                                 1788     svchost.exe    2016-09-06 1
:08:05 UTC+0000
0x3db63ef0         TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING      4        System
0x3db63ef0         TCPv6    :::5357                        :::0                 LISTENING      4        System
0x3dc12510         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING      4        System
0x3dc12510         TCPv6    :::445                         :::0                 LISTENING      4        System
0x3dca6c70         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      484      services.exe
0x3dcbada0         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      484      services.exe
0x3dcbada0         TCPv6    :::49155                       :::0                 LISTENING      484      services.exe
0x3dd16220         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      492      lsass.exe
0x3dd16220         TCPv6    :::49156                       :::0                 LISTENING      492      lsass.exe
0x3dd16340         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      492      lsass.exe
0x3d8f2cf0         TCPv4    -:49208                        192.168.180.255:80   CLOSED         328      svchost.exe
0x3d929750         TCPv4    -:5357                         192.168.180.1:56039  CLOSED         4        System
0x3dada6e0         TCPv4    127.0.0.1:5357                 127.0.0.1:49246      CLOSED         4        System
0x3db615b0         TCPv4    -:0                            72.135.185.14:0      CLOSED         996      svchost.exe
0x3db61b30         TCPv6    -:0                            4887:b90e:80fa:ffff:4887:b90e:80fa:ffff:0 CLOSED          996      svchos
.exe
0x3db63010         TCPv4    127.0.0.1:5357                 127.0.0.1:49248      CLOSED         4        System
0x3dbec910         TCPv4    192.168.180.131:49212          192.168.1.100:8080   ESTABLISHED    1424     5:2878BK [illegible]
0x3de8e010         UDPv4    0.0.0.0:3702                   *:*                                 1788     svchost.exe    2016-09-06 1
:08:05 UTC+0000
0x3de8e010         UDPv6    :::3702                        *:*                                 1788     svchost.exe    2016-09-06 1
:08:05 UTC+0000
0x3deb01e0         UDPv4    0.0.0.0:52816                  *:*                                 996      svchost.exe    2016-09-06 1
:08:05 UTC+0000
0x3deb01e0         UDPv6    :::52816                       *:*                                 996      svchost.exe    2016-09-06 1
:08:05 UTC+0000
```

Рис. 2. Сетевая активность выполняющихся процессов в оперативной памяти

```
root@siftworkstation:~# vol.py -f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.4
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000d230 0x0000000027204230 [no name]
0xfffff8a000024010 0x000000002720f010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000521f0 0x00000000272bd1f0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0002b4010 0x000000002171b010 \??\C:\Users\Client\ntuser.dat
0xfffff8a000d1a010 0x000000001e912010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000d6d010 0x0000000015aa0010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000e48010 0x000000001cba2010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a000fe2010 0x0000000016404010 \SystemRoot\System32\Config\SECURITY
0xfffff8a00102a410 0x0000000015a46410 \SystemRoot\System32\Config\SAM
0xfffff8a0010e9010 0x0000000014ec8010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001177010 0x0000000014eb4010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a001622410 0x0000000006653410 \??\C:\Users\Client\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a001d3a010 0x0000000000200010 \??\C:\System Volume Information\Syscache.hve
root@siftworkstation:~#
```

Рис. 3. Результат ввода команды

На последнем этапе необходимо ввести команду:
vol.py –f /home/sansforensics/Desktop/ram.vmem --profile=Win7SP1x64 malfind
для просмотра кода выполняющегося процесса 5:2878BK (см. рис. 4).

```
Process: 5:2878BK [illegible] Pid: 1424 Address: 0x2550000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 99, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02550000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x02550010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x02550020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x02550030  00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00   ................
```

```
Process: 5:2878BK [illegible] Pid: 1424 Address: 0x610000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 241, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00610000  4d 5a e8 00 00 00 00 5b 52 45 55 89 e5 81 c3 62   MZ.....[REU....b
0x00610010  17 00 00 ff d3 81 c3 97 82 0e 00 89 3b 53 6a 04   ............;Sj.
0x00610020  50 ff d0 00 00 00 00 00 00 00 00 00 00 00 00 00   P...............
0x00610030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00   ................
```

Рис. 4. Просмотр кода процесса 5:2878BK

Как мы видим, внутри исполняемого кода содержится заголовок «MZ». Это говорит о том, что данный код выполняет функции стандартного файла с расширением *.exe. По сути говоря, на этом автоматизированный метод подходит к концу. Далее начинается ручной разбор кода данного процесса. Например, здесь вполне можно установить путем дизассемблирования, что часть кода данного процесса в промежутке от 4d до 00 включает в себя команды, указанные на рис. 5.

```
.data:00000000  4d                  dec ebp
.data:00000001  5a                  pop edx
.data:00000002  e800000000          call loc_00000007
.data:00000007  5b                  pop ebx
.data:00000008  52                  push edx
.data:00000009  45                  inc ebp
.data:0000000a  55                  push ebp
.data:0000000b  89e5                mov ebp,esp
.data:0000000d  81c362170000        add ebx,0x1762
.data:00000013  ffd3                call ebx
.data:00000015  81c397820e00        add ebx,0xe8297
.data:0000001b  893b                mov DWORD PTR [ebx],edi
.data:0000001d  53                  push ebx
.data:0000001e  6a04                push 0x4
.data:00000020  50                  push eax
.data:00000021  ffd0                call eax
.data:00000023  0000                add BYTE PTR [eax],al
.data:00000025  0000                add BYTE PTR [eax],al
.data:00000027  0000                add BYTE PTR [eax],al
.data:00000029  0000                add BYTE PTR [eax],al
.data:0000002b  0000                add BYTE PTR [eax],al
.data:0000002d  0000                add BYTE PTR [eax],al
.data:0000002f  0000                add BYTE PTR [eax],al
.data:00000031  0000                add BYTE PTR [eax],al
.data:00000033  0000                add BYTE PTR [eax],al
.data:00000035  0000                add BYTE PTR [eax],al
.data:00000037  0000                add BYTE PTR [eax],al
.data:00000039  0000                add BYTE PTR [eax],al
.data:0000003b  00f8                add al,bh
.data:0000003d  0000                add BYTE PTR [eax],al
.data:0000003f  00                  .byte 0x0
```

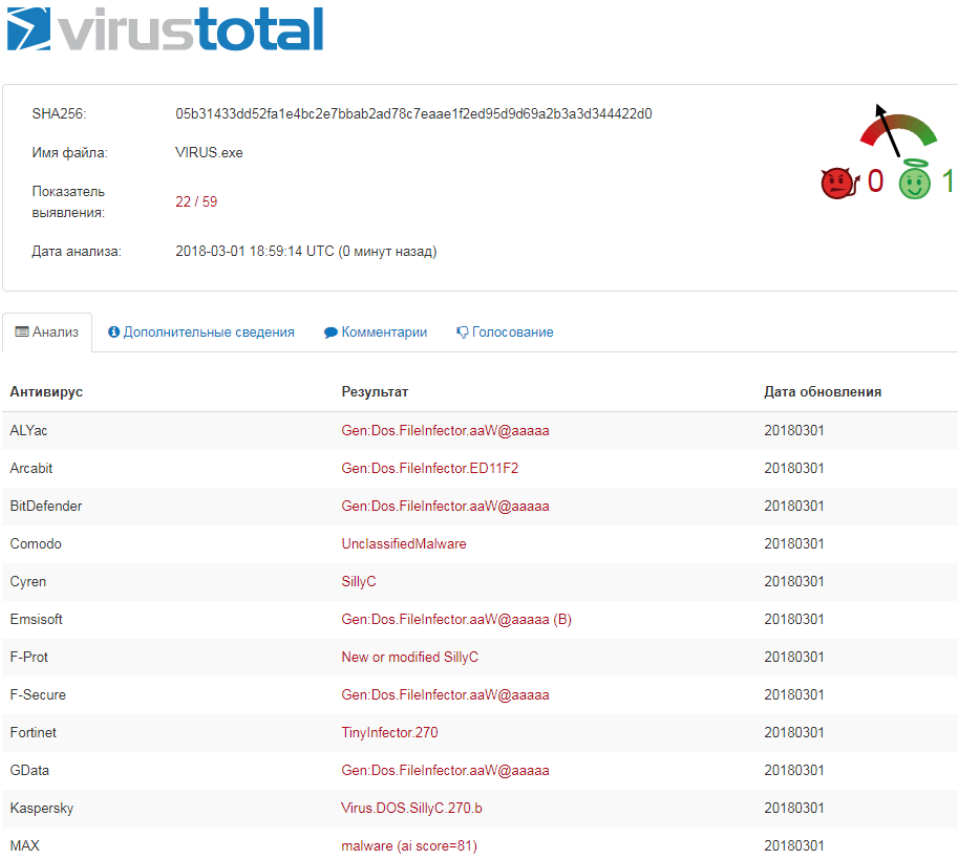
Рис. 5. Результат дизассемблирования части кода процесса 5:2878ВК

Метод проведения исследования, основанный на использовании языка программирования «Assembler». В ходе проведения исследования были использованы: дамп оперативной памяти (файл 20171118.mem); вредоносное программное обеспечение (файл VIRUS.exe, код которого приведен в приложении 1); антивирусное программное обеспечение (онлайн-сервис VirusTotal); виртуальная машина (Oracle VM VirtualBox); операционная система (Windows XP); дизассемблер (IDA Pro Advanced); отладчики – OllyDBG, Emu8086 и AFD Pro; HEX-редактор (WinHex).

Допустим, перед экспертом поставлен вопрос: Детектируется ли представленный на исследование файл VIRUS.exe программой типа «антивирус» как вредоносный? Если да, то производился ли его запуск в операционной системе пользователя?

Чтобы ответить на данный вопрос, для начала необходимо просканировать файл VIRUS.exe каким-нибудь антивирусным программным обеспечением, которое подтвердило бы, что данный файл действительно является вредоносным. В качестве примера сканирование про-

изводилось с использованием онлайн-сервиса VirusTotal, результат выполнения которого отражен на рис 6–8.



virustotal

SHA256: 05b31433dd52fa1e4bc2e7bbab2ad78c7eaae1f2ed95d9d69a2b3a3d344422d0

Имя файла: VIRUS.exe

Показатель выявления: 22 / 59

Дата анализа: 2018-03-01 18:59:14 UTC (0 минут назад)

0 1

Анализ | Дополнительные сведения | Комментарии | Голосование

Антивирус	Результат	Дата обновления
ALYac	Gen:Dos.FileInfector.aaW@aaaaa	20180301
Arcabit	Gen:Dos.FileInfector.ED11F2	20180301
BitDefender	Gen:Dos.FileInfector.aaW@aaaaa	20180301
Comodo	UnclassifiedMalware	20180301
Cyren	SillyC	20180301
Emsisoft	Gen:Dos.FileInfector.aaW@aaaaa (B)	20180301
F-Prot	New or modified SillyC	20180301
F-Secure	Gen:Dos.FileInfector.aaW@aaaaa	20180301
Fortinet	TinyInfector.270	20180301
GData	Gen:Dos.FileInfector.aaW@aaaaa	20180301
Kaspersky	Virus.DOS.SillyC.270.b	20180301
MAX	malware (ai score=81)	20180301

Рис. 6. Результат сканирования файла VIRUS.exe с использованием онлайн-сервиса VirusTotal

McAfee-GW-Edition	Bumah.276	20180301	CMC	✓	20180301
Microsoft	Virus:DOS/Trivial.based.270	20180301	CrowdStrike Falcon (ML)		20170201
eScan	Gen:Dos.FileInfector.aaW@aaaaa	20180301	Cybereason		None
NANO-Antivirus	Virus.Dos.Gen-Crypt.ccnk	20180301	Cylance		20180301
Qihoo-360	Malware.Radar01.Gen	20180301	DrWeb	✓	20180301
Rising	Virus.Dos.SILLYC.270.b (CLASSIC)	20180301	eGambit		20180301
Symantec	Bloodhound.DirAct!COM	20180301	Endgame		20180301
Yandex	DOS.FileMod.Gen	20180228	ESET-NOD32	✓	20180301
ZoneAlarm by Check Point	Virus.DOS.SillyC.270.b	20180301	Ikarus	✓	20180301
Ad-Aware	✓	20180301	Sophos ML		20180121
AegisLab	✓	20180301	Jiangmin	✓	20180301
AhnLab-V3	✓	20180301	K7AntiVirus	✓	20180301
Alibaba		20180301	K7GW	✓	20180301
Antiy-AVL	✓	20180301	Kingsoft	✓	20180301
Avast	✓	20180301	Malwarebytes	✓	20180301
Avast-Mobile	✓	20180301	nProtect	✓	20180301
AVG	✓	20180301	Palo Alto Networks (Known Signatures)		20180301
Avira (no cloud)	✓	20180301	Panda	✓	20180301
AVware	✓	20180301	SentinelOne (Static ML)		20180225
Baidu	✓	20180301	Sophos AV	✓	20180301
Bkav	✓	20180301	SUPERAntiSpyware	✓	20180301
CAT-QuickHeal	✓	20180301	Symantec Mobile Insight		20180220
ClamAV	✓	20180228	Tencent	✓	20180301

Рис. 7. Результат сканирования файла VIRUS.exe с использованием онлайн-сервиса VirusTotal

TheHacker	✓	20180301
TrendMicro	✓	20180301
TrendMicro-HouseCall	✓	20180301
Trustlook	✓	20180301
VBA32	✓	20180301
VIPRE	✓	20180301
ViRobot	✓	20180301
Webroot	✓	20180301
WhiteArmor	✓	20180223
Zillya	✓	20180301
Zoner	✓	20180301

Рис. 8. Результат сканирования файла VIRUS.exe с использованием онлайн-сервиса VirusTotal

Далее необходимо определить, исходя из имеющегося дампа оперативной памяти, был ли осуществлен запуск файла VIRUS.exe. Для этого мы проведем исследование в два этапа: определим, из каких инструкций состоит файл VIRUS.exe и какие следы он оставляет в памяти в результате их выполнения; произведем поиск оставленных следов вредоносным программным обеспечением в дампе оперативной памяти.

Во время проведения исследования необходимо иметь в виду, что существуют различные методы защиты, используемые злоумышленниками, направленные на недопущение изучения кода и то, что ассемблирование является однонаправленным процессом с потерями [1].

Итак, запускаем виртуальную машину с установленной операционной системой (в нашем случае Windows XP). Открываем файл VIRUS.exe с использованием нескольких отладчиков, например, AFD Pro, OllyDBG, Emu8086 и дизассемблера IDA Pro Advanced.

После исследования кода файла VIRUS.exe можно сказать, что перед нами нерезидентный вирус. Это говорит о том, что сразу же после его исполнения в первом свободном сегменте данные могут быть затерты другой программой. Но, возможно, данный вирус оставил свои следы в области седьмой видеостраницы, которая, как правило, никакой программой не используется для хранения своих инструкций, т. к. обычно любой пользователь по умолчанию работает с нулевой видеостраницей. Итак, открываем HEX-редактор WinHex и выбираем в нем дамп оперативной памяти (файл 20171118.mem). Теперь нам необходимо по сигнатуре файла VIRUS.exe найти тело вируса.

В конечном счете, мы убедились, что файл VIRUS.exe действительно был запущен, о чем свидетельствуют следы в виде определенных сигнатур, оставленные данным файлом в оперативной памяти компьютера (см. рис. 9, 10).

Рис. 9. Результат, полученный в результате поиска файла VIRUS.exe

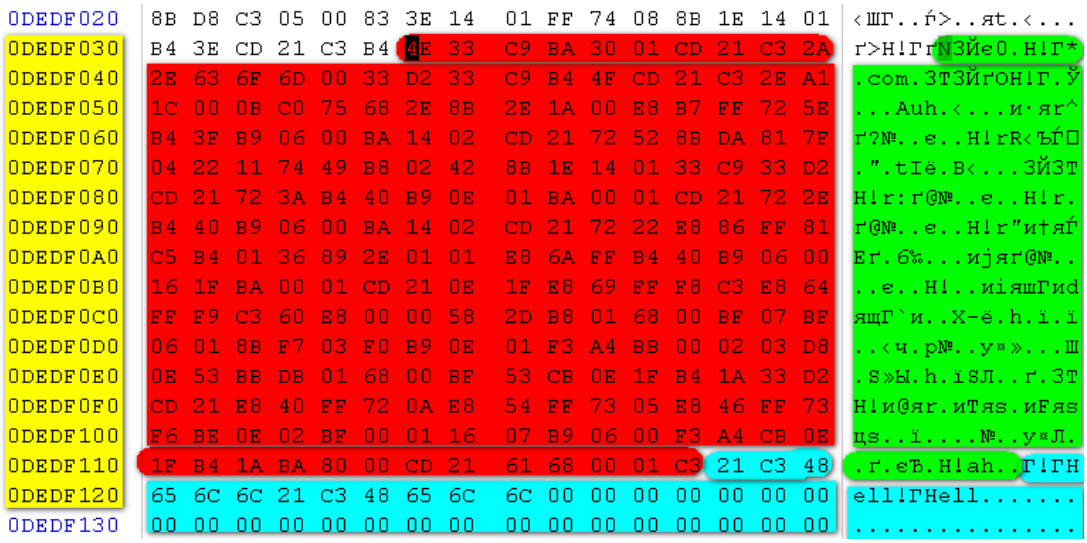


Рис. 10. Результат, полученный в результате поиска файла VIRUS.exe

Библиографический список

1. Климентьев К. Е. Компьютерные вирусы и антивирусы / под ред. Д.А. Мовчана. – М. : ДМК-Пресс, 2015. – С.26-27.

2. BackDoor.Bladabindi.1856 // https://vms.drweb.ru/virus/?i = 4037915 (дата обращения: 19.02.2017).

3. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел. Сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.

В. В. Эльканов[1], Д. Н. Захаров[2], В. Н. Куликов[3]

СРАВНЕНИЕ И АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ

Сравнение и анализ сканеров уязвимостей. Современный мир тесно связаны с использованием информационных технологий, которые в свою очередь подвержены различным угрозам информационной безопасности. Одной из важных задач является выявление рисков и дыр в защите, которыми могут воспользоваться злоумышленники. Решение этой задачи требует комплексного подхода, включающего, в частности, разработку политики безопасности предприятия. Таким образом, специалистам необходимо контролировать и поддерживать состояние защищенности компьютерной сети. В этом им помогают системы анализа защиты или сканеры уязвимости, или по другому сканеру безопасности сети. Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. Грамотно используя сканер уязвимости сети, специалист может значительно усилить сетевую безопасность. Большинство атак происходит через известные и опубликованные «лазейки» безопасности, которые могут быть не ликвидированы по причинам, будь то нехватка времени, персонала или некомпетентность системного администратора. Так как этих «лазеек» может быть несколько, то злоумышленник имеет множество способов проникнуть в систему, а при неудачной попытке использовать другой метод. Именно поэтому данная задача имеет комплексный подход.

Также не стоит забывать, что помимо специалистов сканерами безопасности могут пользоваться и обыкновенные пользователи для защиты своей сети и конфиденциальной информации.

Сканер безопасности – это программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей, которые могут быть использованы посторонними лицами для доступа к конфиденциальной информации и нарушения работы системы вплоть до полной потери данных и работоспособности [1].

---

[1] Курсант факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Эльканов В. В., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Захаров Д. Н., 2018.

[3] Старший преподаватель кафедры Иностранных языков МосУ МВД России имени В.Я. Кикотя. © Куликов В. Н., 2018.

На данный момент рынок сканеров огромен, и каждый производитель обещает широкие спектр возможностей для привлечения внимания пользователей. В данной статье рассматривались спектр возможностей сканера и простота его использования. Для участия в тестовых испытаниях были отобраны сканеры, представленные в таблице:

Название	*Версия*	*Ссылка*
Nessus	7.0.1	http://www.nessus.org/download
MaxPatrol	8	http://www.ptsecurity.ru/maxpatrol.asp
GFIOneGuard	9.6.20101113	https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download?adv=220295&loc=1
OpenVAS	9	http://www.openvas.org/download.html

MaxPatrol. Комплексное программное решение разработчиков компании PositiveTechologies. С помощью MaxPatrol вы можете контролировать защищенность всей ИН-инфраструктуры и оперативно реагировать на все значимые инциденты. Данное программное обеспечение не нуждается в программах агентах на удаленных системах.

MaxPatrol позволяет проводить тестирование на проникновение и оценку приложений, инвентаризацию сетей и проверку сетевого периметра.

Аудит политики паролей методами черного и белого ящика для систем удаленного доступа и VPN, протоколов приложений, настольных приложений, а также систем совместного использования файлов и каталогов. Сетевой аудит способен собирать важную информацию в файлах и базах данных.

Встроенные базы данных для компонентов многих систем позволяют обнаруживать инциденты или нежелательные изменения. Содержат в себе технологию обнаружения небезопасного кода, вредоносного ПО и троянов во всех системах без использования агентов.

Другие дополнительные функции MaxPatrol позволяют создавать единую информационную структуру, которая управляет ресурсами, связью со службой поддержки, управлять рисками, исправлениями и WAF – тестирование на проникновение NAC/NAP.

Также данный продукт обладает русскоязычным интерфейсом [2].

CFI Oneguard. С помощью GFI OneGuard ИТ-Администраторы могут просматривать состояние нескольких сетей, открывать несколько приложений или консолей.

Данная программа предоставляет виджеты панели на антивирусное обслуживание, состояние развертывания управления исправлениями, сетевой аудит и многое другое.

Аудит и развертывание исправлений программного обеспечения в пределах недвижимости являются трудоемкой задачей, которая ни один админ не хочет предпринимать, пока не может избежать. ГФИ OneGuard помогает значительно автоматизировать работы, вы можете быстро оценить уровни программного обеспечения на каждое подключенное устройств и патч соответственно.

ГФИ OneGuard может быть настроен на автоматический пластырь операционных систем, приложений, браузеры и многое другое. Вы устанавливаете уровень исправления, расписание и точные обновления для установки.

Сетевой аудит и отслеживание активов, чтобы эффективно защитить свою сеть, вы должны точно знать, где именно. Вот где входит сетевой аудит. GFIOneGuard может автоматически сканировать и обнаруживать все.

Устройство Windows в любой сети, в любом месте. Централизованный контроль аудит-двигатель будет искать и отчитываться об оборудовании, программном обеспечении и установленных приложениях.

Другие дополнительные функции GFI OneGuard также предоставляет инструменты для обмена сообщениями для трансляции оповещения и информации к потребителям, удаленным возможностям перезагрузки или выключения и полноценной системе отчетности доставить нужную вам информацию в течение нескольких минут [3].

Nessus. Nessus представляет программу для автоматического поиска известных изъянов в защите информационных систем, чтобы выявить уязвимости, политика-нарушение конфигурации и вредоносные программы. Особенности Nessus высокой скоростью обнаружения активов, аудит конфигурации, целевое профилирование, обнаружение вредоносных программ, обнаружение конфиденциальных данных и многое другое.

Nessus поддерживает больше технологий, чем конкурентных решений, сканирование операционных систем, сетевых устройств следующего поколения брандмауэры, гипервизоры, базы данных, вебсерверы и критические инфраструктура для уязвимостей, угроз и соответствия требованиям нарушения.

Nessus производит ранжирование уязвимости на основе CVSS, пять уровней серьезности (критические, высокие, Средние, низкие, Инфо), настраиваемые уровни серьезности для пересчета риска. Настройка отчетов для сортировки по уязвимости или хосту создайте сводка или сравнение результатов сканирования для выделения изменения в формате XML, PDF, HTML и CSV форматы Добавление собственного имени и логотипа в отчет. Автоматизировать загрузку отчетов с помощью API [4]. Open VAS (Open Source Vulnerability Assessment Scanner). Open VAS – это сканер уязвимостей и средство управления уязвимостями с открытым исходным кодом. OpenVAS предназначен для активного мониторинга узлов вычислительной сети на предмет наличия проблем, связанных с безопасностью, оценки серьезности этих проблем и для контроля их устранения. Активный мониторинг означает, что OpenVAS выполняет какие-то действия с узлом сети: сканирует открытые порты, посылает специальным образом сформированные пакеты для имитации атаки или даже авторизуется на узле, получает доступ к консоли управления и выполняет на нем команды. Затем OpenVAS анализирует собранные данные и делает выводы о наличии каких-либо проблем с безопасностью. Эти проблемы в большинстве случаев касаются установленного на узле необновленного ПО, в котором имеются известные и описанные уязвимости, или же небезопасно настроенного ПО [5].

Критерии. Прежде чем выбрать критерии сравнения, следует подчеркнуть, что критерии должны охватывать все аспекты использования сканеров безопасности: начиная от методов сбора информации и заканчивая стоимостью [6]. При работе с сканером первым делом мы обращаем внимание на его архитектуру. Поэтому первая группа критериев охватывает взаимодействия компонентов сканеров, их инсталляции и управления. Вторая группа критериев – сканирование. Данная группа должна охватывать методы, которые используют сканеры, а также результаты сканирования, их отчеты и возможность произвольного формирования отчета. Последние критерии, на которые стоит обратить внимание, это обновления и поддержки, которые помогают выяснеть методы обновлений, а также уровень технической поддержки, и др.

Заключение. В работе были рассмотрены 4 сканера уязвимостей, которые были подвергнуты сравнению по выделенным критериям.

По эффективности лидер был выбран сканер MaxPatrol наиболее полным спектром возможностей для проведения анализа защищенности компьютерной системы.

Библиографический список

1. Никсов Дмитрий, Рудель Петр // Системный администратор. – 2003. – Вып. № 1 (2).
2. Официальный сайт программ // https://docs.tenable.com.
3. Официальный сайт программ // https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-oneguard.
4. Официальный сайт программ // https://www.ptsecurity.com/ru-ru/about/docs.
5. Русскоязычное сообщество пользователей сканера уязвимостей OpenVAS //https://openvas.ru.

А. В. Никифоров[1], Д. А. Кравченко[2]

ФИКСИРОВАНИЕ ВЕРБАЛЬНЫХ ПРОЯВЛЕНИЙ КЛЮЧЕЙ ДОСТУПА К СКРЫТОЙ ИНФОРМАЦИИ КАК СПОСОБ РАЗОБЛАЧЕНИЯ ЗАМЫСЛА КИБЕРПРЕСТУПНИКОВ

Электронная сеть «Интернет» неотъемлемая часть современного государства, но за каждым из электронных устройств находится человек. От взаимоотношений, существующих в различных формах и проявлениях зависит развитие бизнеса, экономики страны и порой обороноспособности Родины.

Актуальность темы в сфере киберпреступлений очевидна, так для клиента крайне важно знать реальную картину как о качестве товара, поставляемого ему, так и честность того человека, сотрудничающего по ту сторону экрана. Психолог, используя современные вербальные ключи доступа к скрытой информации в речи, в состоянии распознать истинные намерения партнера для принятия решения о развитии деловых отношений с ним.

Большинство исследований по психологии лжи затрагивают проблемы намеренного искажения информации в межличностном общении (П. Экман, А. Пиз, В. В. Знаков и др.). Объектно-предметной областью нашего анализа является малоизученная проблема самообмана человека. Мы предположили, что более глубокое понимание вербальных ключей доступа к скрытой информации и знание механизмов са-

---

[1] Преподаватель кафедры психологии Военного университета Министерства обороны Российской Федерации. © Никифоров А. В., 2018.

[2] Курсант 943 учебной группы факультета Морально-психологического обеспечения войск Военного университета Министерства обороны Российской Федерации. © Кравченко Д. А., 2018.

мообмана, проявляющихся в речи военнослужащих, позволят качественно осуществлять психологическое сопровождение их служебной деятельности.

В Оксфордском словаре английского языка говорится: «В современном употреблении слова (ложь) обычно имеется оттенок ярко выраженного морального осуждения, и в вежливой беседе его стараются избегать, часто заменяя такими синонимами, как «обман» и «неправда», имеющими относительно нейтральное звучание» [1]. Однако Пол Экман термины «ложь» и «обман» использует как синонимы.

При определении лжи мы должны брать во внимание не только того, кто лжет, но и, конечно, жертву обмана. Ведь во время акта лжи, жертва не просит, чтобы ее ввели в заблуждение, да и сам лжец не предупреждает о том, что будет говорить неправду.

И как пишет в своей книге Пол Экман: «*Определяет ложь (или обман), как действие, которым один человек вводит в заблуждение другого, делая это умышленно, без предварительного уведомления о своих целях и без отчетливо выраженной со стороны жертвы просьбы не раскрывать правды*» [2].

Что касается нашего отечественного автора Знакова В. В. по данной теме, то он пишет следующее: «В последнее время в гуманитарных науках наблюдается лавинообразное нарастание интереса к проблемам понимания сущности правды и ее психологических антиподов – лжи, обмана и неправды» [3].

Так, для квалификации неправды как категории психологии взаимопонимания нам прежде всего необходимо определить, в какой степени мысли военнослужащего о действительности соответствуют самой действительности. Иначе говоря, следует признать модель мира военнослужащего верной или ошибочной.

Пол Экман выделяет следующие основные формы лжи:

1. Умолчание. При умолчании лжец скрывает истинную информацию, но при этом не сообщает ложной.

2.Искажение. При искажении же лжец предпринимает некие дополнительные действия – он не только скрывает правду, но и преподносит взамен ложную информацию, выдавая ее за истинную.

3. Когда лжец просто не говорит всей правды, т. е. не договаривает.

4. Когда лжец говорит правду так, что ему не верят.

5. Сбивающая с толку увертка.

Теперь что касается нашего отечественного психолога В. В. Знакова вот что он думает на этот счет.

Неправда в средствах массовой информации и ситуациях межличностного общения обычно проявляется в двух разновидностях.

Во-первых, неправда как вербальный эквивалент заблуждения: человек верит в реальность существования чего-то, но ошибается – в результате он говорит неправду, сам того не осознавая. Так, спортсмен в кругу друзей может рассказывать, что его соперник перед соревнованиями употребляет допинг.

Во-вторых, неправда как следствие ограниченности знания, неполноты истины: описание говорящим внешней стороны поступка другого человека при незнании мотивов последнего и конкретных обстоятельств, в которых реализуется поведение. В социальном познании правдивыми следует считать только такие сообщения о поведении людей, в которых отражены все три основных компонента любого поступка – действие, его цель и внешние условия. В противном случае данных, необходимых для адекватного понимания поступка, оказывается недостаточно. Обычно это приводит к искажению реальной картины описываемых событий в сознании понимающего субъекта и, следовательно, превращению правды в неправду.

Прежде всего, хочется сказать, что ложь, как один из человеческих факторов, закладывается с детства, причем на ранних его этапах.

Теперь что касается самих причин лжи и обмана. У разных авторов, будь это зарубежный или же какой-либо отечественный ученый, имеется свое мнение на этот счет. В психологии речи наблюдается большое разнообразие методов и приемов исследований. Известно, что методы исследований в науке или научной области тесно связаны с ее предметом. Интересующая нас область не составляет исключения. В связи с этим различны и исследовательские подходы.

Один из них базируется на идее, согласно которой предметом психологического исследования следует считать речь, но не язык, относящийся к социальным явлениям.

В своей работе мы рассматриваем ложь, как одну из самых распространенных форм скрытия информации.

Возникает закономерный вопрос: Почему же ложь не единственный метод скрытия информации? Ответ на него закономерен и прост, поскольку даже когда мы молчим, не говоря ни слова, когда нас о чем-либо спрашивают, а мы специально, подчеркиваю, специально молчим, мы уже тогда скрываем какую-либо информацию.

Другой случай, когда мы скрываем информацию ни слова не сказав лжи – банальная смена разговора, уход от темы, для скрытия той ин-

формации, которую хочет знать наш собеседник [4]. И последний пример скрытия информации без лжи – это корректный отказ от дачи информации. Так, как сказав вежливо «нет», мы в одно и то же время скрыли информацию, при этом ни солгав, ни слова. Говоря о лжи, как форме скрытия информация, мы использовали классификацию В. В. Знакова.

Правда и ее строгая противоположность – ложь, характеризуется по трем основным признакам: фактическая истинность или ложность утверждения; вера говорящего в истинность или ложность утверждения; наличие или отсутствие у говорящего намерения ввести в заблуждение слушающего. Перечисленные три признака дают основания для классификации разновидностей правды и психологического анализа ее отличий от семантических антиподов (неправды, лжи, обмана и др.). В табл. 1 представлены результаты анализа.

С точки зрения психологии общения и взаимопонимания самообман представляет собой особый случай внутреннего диалога, аутокоммуникации: здесь и обманывающий, и обманываемый представлены в одном лице. Наиболее очевидные ситуации, ведущие к самообману, обычно связаны с тем, что человек, получая какое-то знание, не верит в его правдоподобие или вовсе отрицает, отторгает от себя.

Таблица 1.

Классификации разновидностей правды и психологического анализа ее отличий от семантических антиподов неправды, лжи и обмана В. В. Знакова

Соответствие или несоответствие высказывания фактам	Утверждение говорящего соответствует фактам		Утверждение говорящего, не соответствует фактам		
Намерение обмануть партнера	Говорящий верит в истинность утверждения	Говорящий не верит в истинность утверждения	Говорящий верит в истинность утверждения	Говорящий не верит в истинность утверждения	
Говорящий не имеет намерения обмануть партнера	1. Правда	2. Правда	3. Неправда	4. Неправда	5. Вранье
Говорящий имеет намерение обмануть партнера	6. Обман	7. Мнимая ложь	8. Самообман	9. Ложь	

Ключи доступа скрытой информации можно выделить из вышеприведенной классификации в частности из 8 клетки.

С точки зрения психологии общения и взаимопонимания самообман представляет собой особый случай внутреннего диалога, аутокоммуникации: здесь и обманывающий, и обманываемый представлены в одном лице В. В. Знаков описывая содержательную сторону самообмана, фиксирует, что в западной психологической традиции понятие «самообман» не используется. Исследование самообмана в зарубежной психологии проходит в рамках изучения защитных механизмов личности.

В психологических словарях защитный механизм определяется как способ устранения или сведения к минимуму негативных переживаний, сопряженных с внутренними или внешними конфликтами, состояниями тревоги и дискомфорта. П. Экман в своем исследовании отмечает, что ядром лжи является ее эмоциональный компонент. Именно благодаря повышению интенсивности переживания в момент лжи позволил П. Экману разработать приемы и способы ее диагностики. Исходя из этой логики, ядром самообмана так же является переживание.

Рассматривая защитный механизм вытеснение, как прием самообмана, можно задаться вопросом: куда же вытесняется наше переживание, от нашего сознания тревога прячется в бессознательном, т. к. бессознательное, по определению З. Фрейда, это животная составляющая человеческой психики [5].

Также подобная защита довольно затратная для психики человека, поскольку переживание подобно поплавку на глади воды, если не затрачивать силы на «утопление» поплавка, то он будет выныривать все снова и снова. Также и переживание, «утопленное» в пучину бессознательного, будет постоянно напоминать о себе, если на него не затрачивать психические силы для удержания переживания в бессознательном.

Из вышесказанного можно выделить то, что, в конечном счете, подобный защитный механизм вынуждает отказаться от него, возвращая былой дискомфорт.

Для упрощенного восприятия информации и легкого усвоения данные, изложенные выше, представлены в виде табл. 2.

Таблица 2.

Защитные механизмы и их проявление в речи

Защитный механизм	*Суть*	*Проявление*
Вытеснение (repression)	Заключается в активные устранения источника угрозы из сферы сознания, препятствующие воспроизведению информации, прямо или ассоциативно связанной с психотравмирующим опытом	Скрываемая информация прорывается «наружу» в шутках, оговорках, и т.д.
Отрицание (denial)	Результат которого осуществляется как попытка непринятия источника угрозы, как реального события	Нарушение логики повествования. Разрушение логики и морали. «…где логические ошибки, там и проблемы»
Рационализация (rationalization)	Это поиск допустимых причин для недопустимых мыслей или действий	Оправдание своих действий. Человек бессознательно изобретает логичные суждения и умозаключения для объяснения своих неудач. Подчеркивание проблемы чрезмерными двойными отрицаниями и пр. Творческое мышление и т.д.
Проекция (projection)	Приписывание другому лицу, животному или предмету качеств, чувств или намерений, которые коренятся в самом человеке	Проявление данного механизма можно выразить фразой: «В своем глазу бревна не видишь, а в чужом щепку замечаешь»
Регрессия (regression)	Форма психологического приспособления в ситуации конфликта или тревоги, когда человек бессознательно прибегает к более ранним, менее зрелым и менее адекватным образцам поведения, которые кажутся ему гарантирующими защиту и безопасность	Демонстрация болезненности, ущербности и др. также относится к регрессии, т. к. содержит то же послание: «Я больной, я не способен о себе позаботиться, защитите меня». Истеричный тон голоса. В речи проявляется посредством истеричного тона голоса, повышения голоса (крик), конючения

Для создания ситуации, в которой мы подвергнем нашего партнера проверке на истинность мотивов, вызванных сотрудничеством с нами необходимо создать ситуацию, которая не предполагалась им, той ситуации, когда его же защитные механизмы начнут нам сигнализировать о попытке обмануть нас.

Для создания такой ситуации стоит изучить стандартные схемы киберпреступников введения в заблуждение своих жертв и якобы попасться на их уловку, но в момент практически свершенной сделки предъявить ту или иную схему для введения собеседника в состояние фрустрации. Именно в таком состоянии психика человека начнет защищаться от негативных ощущений и вышеперечисленные «симптомы» той или иной защиты начнут проявляться, вследствие чего можно будет усомниться в честности нашего партнера.

Нами приведен один из примеров практического применения таблицы механизмов защиты, ее же можно применять и в других ситуациях, главное внимательно наблюдать за их проявлениями.

В заключение делаем вывод, что при помощи должного обращения внимания на речь, прислушивания к своему собеседнику, человек может выявить вышеперечисленные признаки защитных механизмов и использовать их для правильного понимания доносимой информации высказывания.

К тому же, человек может избежать обманывания себя даже при том, когда собеседник верит или пытается верить в ту информацию, что доносит, а порой и выявить что беспокоит человека грамотно поступить в той или иной ситуации.

Для руководителя и психолога крупных предприятий вышеперечисленные проявления защитных механизмов рекомендуется знать наизусть и постоянно применять их на практике, анализировать речь партнеров и сотрудников для избегания обманывания и правильного принятия решения.

Кроме того, вышеуказанные признаки речевого самообмана могут помочь выявить различные отклонения как в психическом, так и физическом здоровье.

Данные анализа рекомендуется использовать не только для выявления искренности высказывания людей, но и для внутреннего самоанализа в целях более эффективной работы над собой, потому что, фиксируя самообман, мы можем сосредоточится на главной цели, отбрасывая лишнее слова, поступки.

Библиографический список

1. Оксфордский словарь английского языка.
2. Экман Пол Психология лжи. – Питер, 2007. – 307 с.
3. Знаков В. В. Психология понимания правды. – СПб., 1999.
4. Фрейджер Р., Фэйдимен Д. Теории личности и личностный рост. – СПб. : Прайм-Еврознак, 2004. – 608 с.
5. Никифоров А. В., Кравченко Д. А. Анализ психологических подходов к проблеме вербальных ключей доступа к скрытой информации: материалы конференции психология служебной деятельности сотрудников. – М. : МосУ МВД России имени В.Я. Кикотя, 2017.

А. В. Козырев[1], В. Ю. Иванов[2], А. О. Путилов[3]

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ RAID-МАССИВОВ ДАННЫХ

В данной статье рассмотрены основы по исследованию RAID-массивов данных. Рассмотрена история создания, понятийный аппарат, классификация и принципы работы наиболее популярных видов RAID-массивов, а также были рассмотрены проблемы, возникающие у правоохранительных органов при работе с данным устройством.

В современном мире роль информации возрастает с каждым днем все больше и больше. Информацией пользуются все население земного шара и жизни без нее они не видят. Информацией пользуются так же и злоумышленники для того, чтобы причинить вред другим людям, ради получения любого вида благополучия будь то материальное, будь то информационное или любое-другое. А злоумышленники скапливают информацию у себя и хранят ее у себя до того момента, когда нужно будет – применят ее. Информационные технологии шагают вперед. Поэтому устройства хранения данных изменяются, прогрессируют, и становятся все более надежными хранилищами для информации. Устройства хранения данных позволяют защитить любые важные данные сервера и сохранить их для последующего извлечения. Если у

[1] Слушатель 518 учебного взвода 5 «И» курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Козырев А. В., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Иванов В. Ю., 2018.

[3] Преподаватель кафедры информатики и математики МосУ МВД России имени В.Я. Кикотя. © Путилов А. О., 2018.

вас нет высоких требований к избыточности или производительности, вам вполне подойдет один диск. В противном случае можно использовать RAID [2].

Первый НЖМД, который назывался IBM 350, в лаборатории был собран 10 января 1955 г. американской компанией IBM. Размеры данного жесткого диска были сравнимы с размерами хорошего шкафа для одежды, а вес его был около тонны, но при всем своем «величии» имел очень маленький объем записываемой информации – всего 5 мегабайт. В нынешнее время такой объем считается очень крохотным и слишком смешной, но на фоне того что до тех пор использовались магнитные ленты с последовательным доступом и перфокарты это был огромный прорыв в технологической индустрии.

Но как бы там не было печально, ведь особенности той самой технологии являются причиной появления двух основных проблем, связанные с пользованием НЖМД. Одной из них является то, что скорость чтения/записи и взаимосвязи между жестким диском и процессором слишком низка.

Второй проблемой является низкая защищенность информации, которая может храниться на винчестере.

Но есть методы, которые могут помочь снять выше перечисленные проблемы обычных жестких дисков. Одним из таковых является сборка RAID–массивов, состоящих из двух и более НЖМД.

В 1987 г. американские ученые-исследователи Калифорнийского университета Беркли описали и предложили такой подход по объединению дисков в единую систему. Паттерсон, Гибсон и Катц в своей статье «A Case for Redundant Arrays of Inexpensive Discs, RAID» («избыточный масссив недорогих дисков») описали принцип объединения двух и более недорогих винчестеров в единое логическое устройство, при этом в результате данное устройство увеличивало объемы хранения и ускоряло работу системы, а отказ одного из нескольких НЖМД не мог привести к отказу в работе всей системы.

С тех времен прошло уже порядка 15 лет, но предложенная технология сборки RAID-массивов все также актуальна на сегодняшний день. Изменения претерпела лишь расшифровка аббревиатуры RAID – слово Inexpensive (недорогие) поменяли на Independent (независимые), что больше походило на правду. Причиной тому является тот факт, что изначально RAID-массивы создавались на далеко недешевых дисках.

RAID (англ. – redundant array of independent disks– избыточный массив независимых жестких дисков) – массив из нескольких дисков под управлением контроллера, связанных друг с другом высокоскоростными каналами связи и представляющих единое целое для всей системы.

Увеличение производительности подсистемы дисков строится на одновременной работе нескольких НЖМД, т. е. чем больше винчестеров в массиве (но до определенного предела), тем лучше.

Существует два вида организации работы НЖМД в массиве: параллельный доступ; независимый доступ.

В нынешнее время существует достаточное разнообразие видов (или по-другому «уровни») RAID-массивов: 0, 1, 2, 3, 4, 5, 6, 10. Наиболее распространенными являются 0, 1, 2, 5. Для дальнейшего рассмотрения проблем необходимо рассмотреть самые распространенные виды RAID-массивов.

RAID 0. Дисковый массив без отказоустойчивости (Striped Disk Array without Fault Tolerance).

Данный уровень представлен массивом дисков с разбивающемся на блоки данными, каждый из которых будет читаться/записываться на определенный отдельный диск. Все это в конечном счете будет способствовать проведению нескольких операций чтения/записи в один и тот же период.

RAID 1. Дисковый массив с дублированием или зеркалка (mirroring).

Зеркалирование – это есть стандартный способ для увеличения надежности массива дисков относительно небольшого объема. Простым языком этот массив строится на основе двух НЖМД, на которых будет записываться абсолютно одинаковая информация. Тем самым будет создаваться «зеркало» основного диска. То есть при утрате работоспособности одного из дисков другой будет продолжать работать в стандартном режиме, без каких-либо сбоев и тем более потерь информации.

RAID 2. Отказоустойчивый массив дисков с применением кода Хемминга (Hamming Code ECC).

Уровень RAID 2 использует в своем действии код Хемминга, который исправляет как одиночные, так и двойные неисправности массива. Данный метод сейчас активно применяется в технологии кодирования информации в оперативной памяти типа ECC.

RAID 5. Отказоустойчивый массив независимых дисков с распределенной четностью (Independent Data disks with distributed parity blocks).

Данный уровень имеет схожесть с RAID 4, но отличается циклическим распределением четности по всему дисковому массиву. Это отличие дало увеличение производительности чтения/записи малых объемов данных в системе с большим количеством запросов. Если операции чтения/записи спланировать правильно, то появится возможность параллельным образом обрабатывать до N/2 блоков, где N– число дисков в группе.

Проблемы, возникающие при производстве следственных действий с данными объектами. Сложности при использовании злоумышленниками RAID-массивов возникают у правоохранительных органов. Ибо происходит очень много ошибок и в дальнейшем проблем с проведением изъятий, выемок и проведения исследований и экспертиз, а также осмотров. Это вызвано большим числом факторов.

Во-первых, большинство сотрудников правоохранительных органов не знают, что такое RAID-массив, как он работает, для чего он необходим, как его применять и как им пользоваться.

Во-вторых, исходя из первого фактора образуется следующий фактор отсутствия знаний по изъятию и выемки данного устройства у злоумышленников при производстве обысков или при проведении оперативно-разыскного мероприятия «Обследование помещений, зданий, сооружений, участков местности и транспортных средств». Знания отсутствуют из-за отсутствия каких-либо методических рекомендаций по проведению выемки/изъятия такого рода устройств.

Из-за отсутствия методических рекомендаций по изъятию/выемки RAID-массивов совершается большое количество ошибок, что приводит к осложнению и затруднению проведения, а иногда и к полной невозможности выполнения исследования или компьютерно-технической экспертизы экспертно-криминалистическими центрами системы МВД России. Чаще всего изымают просто весь комплект жестких дисков и в протокол их прописывают как независимые магнитные жесткие диски. Но, изымая по отдельности каждый винчестер, нарушается вся связанность друг с другом данных дисков, что приводит к нарушению работоспособности этих дисков в единой системе и, как следствие, RAID-массива в целом. Ведь чтобы вынуть всю информацию из RAID-массива, он должен работать как система, а не как куча беспорядочных дисков (НЖМД).

Одной из главных проблем является то, что в самих экспертно-криминалистических центрах системы МВД России отсутствуют методические рекомендации по производству исследований и экспертиз RAID-массивов. Да, есть типовые методики по исследованию и экспертизе независимых жестких магнитных дисков. Но в RAID-массиве они уже не независимые и работают они совсем по-другому, во взаимодействии друг с другом с различной вариацией хранения информации на них в зависимости от вида RAID-массива. Так, самое главное нет никаких методик о том, как восстанавливать информацию, какими средствами и какое программное обеспечение для этого использовать. Да, есть знания у самих экспертов о том, что если привезли RAID-массив в каком-либо виде, то нужно сначала его собрать в необходимый порядок, после этого попытаться восстановить сначала работоспособность RAID-массива, а потом уже и всю информацию с него.

И еще одной проблемой является отсутствие RAID-контроллеров различных типов. Ибо чаще всего изымают только жесткие диски, а не весь RAID-массив в сборе. При сборке их в ЭКЦ будут необходимы контроллеры, а их нет или есть, но в маленьком количестве и только для популярных видов RAID-массивов.

Вот такой список проблем возникает при работе правоохранительных органов в производстве обысков, исследований и экспертиз.

Библиографический список

1. Клыга А. RAID-массивы в теории и на практике [Электронный ресурс] – URL: http://www.progzona.narod.ru/partitions/articles/different/raid_ mass_on_teor_pract.html (дата обращения: 23.11.2017).

2. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел. Сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.

А. М. Тимофеева[1], *В. Ю. Иванов*[2]

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПОД ОС ANDROID

В настоящее время наблюдается широкий рост популярности мобильных устройств. Дружественный интерфейс, простота, финансовая доступность, беспроводной доступ и вместе с тем широкие возможности мобильных устройств дали их повсеместное распространение среди людей разных поколений. Сейчас мобильный телефон есть практически у каждого человека на планете. Требование к знаниям и навыкам пользователей существенно снизились, и теперь уже 64 % пользователей Интернета выходят в сеть при помощи мобильных устройств [1].

В современном мире мобильные устройства с нами всегда и в отличие от компьютера в нем куда больше возможностей для получения разного рода информации о пользователе, например, биометрическая информация, запись звука с телефона, запись фото, видео и определение местоположения.

Кроме того, существует ряд возможностей мобильного телефона, с помощью которых вредоносные программы могут влиять на функционирование устройства, начиная от инициирования платных звонков и СМС-сообщений, заканчивая атаками на банк-клиенты и технологиями бесконтактных платежей. Таким образом, эти факторы является предпосылками к росту преступлений в сфере использования информационных технологий. Лаборатория Касперского постоянно проводит мониторинг активности вредоносного программного обеспечения, в том числе и на мобильных устройствах [5].

На диаграмме представлен период с третьего квартала 2016 г. по второй квартал 2017 г. [2] (рис. 1). Видна тенденция по снижению числа распространившихся вредоносных программ, однако общее количество обнаружений за второй квартал 2017 г. все равно остается на высоком уровне, ведь это более 1,3 млн мобильных устройств. Поэтому исследование вредоносных программ для мобильных устройств является сейчас приоритетной задачей.

---

[1] Слушатель 518 учебного взвода 5-И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Тимофеева А. М., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Иванов В. Ю., 2018.

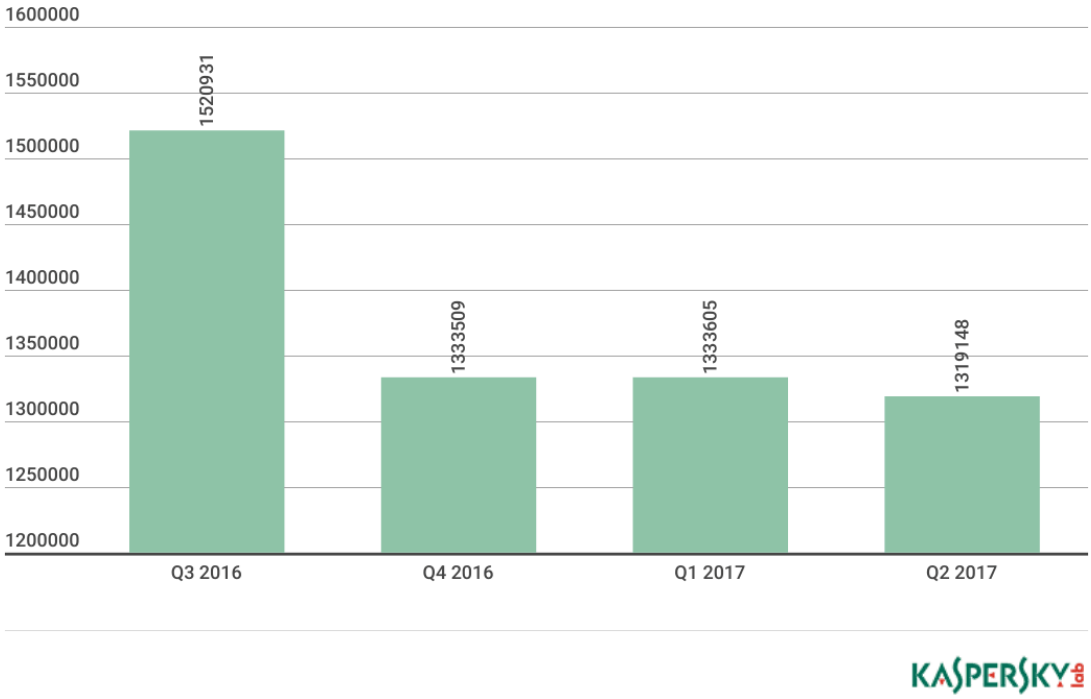


Рис. 1. Статистика количества обнаруженных вредоносных установочных пакетов

В целом существует два метода анализа вредоносного программного обеспечения, а именно: статический и динамический [3].

Статический используется, когда производится поиск вредоносного кода внутри подозрительного приложения, т. е. производится обратное проектирование установщика или исполняемого файла программа до уровня исходного кода. Однако данный метод требует определенных навыков, знаний и опыта для точного определения, заложенного в программу алгоритма [4].

Этапы проведения статистического исследования подозрительного программного обеспечения в операционной системе Android:

1. Необходимо любым архиватором, например 7zip или WinRar, распаковать APK файл.

2. Используя инструмент Dex2jar, необходимо провести конвертацию скомпилированного файла Android формата «Dalvik Executable» (расширение «.dex») в формат Jar «Java ARchive».

3. Полученный файл является стандартным java приложением, поэтому используя инструмент Java Decompiler, можно просмотреть исходный код и существующие классы.

Произвести анализ полученного исходного кода.

Во время динамического анализа проверяется поведение приложения, для этого подозрительную программу запускают в так называемой «песочнице», виртуальной машине или устройстве. Иными сло-

вами, в «безопасной среде», где подозрительная программа не сможет нанести ущерб исследователю.

Непосредственно анализ заключается в записи и анализе событий происходящих с программой во время ее запуска, таких как: операции с файлами, доступ к определенным опасным функциям устройства (отправка смс, включение микрофона и т. п.), обращение в сеть «Интернет» и содержание принятых и отправленных сетевых пакетов.

Этапы динамического анализа подозрительного программного обеспечения в операционной системе (один из возможных подходов для анализа):

1. Необходимо запустить инструмент контроля, например «Snort» от компании «Cisco System», который позволяет определить вторжение и «опасное поведение» программы.
2. Выполнить установку подозрительного программного обеспечения в тестовую «безопасную среду» (например, запустить в «Android Emulator»).
3. Запустить подозрительное ПО (события, происходящие в Android Emulator, уже фиксируются на данном этапе).
4. Отследить все сетевые соединения.
5. Произвести анализ полученных данных.

Оба метода имеют свои плюсы и минусы. Выбор того или иного зависит исключительно от решения и опыта аналитика. В большинстве случаев динамический анализ предоставит результаты намного быстрее, чем статический, несмотря на то, что некоторые вещи могут быть упущены, хотя и легко определяются во время статического анализа.

Определившись с методами исследования, необходимо определить существующие практические средства для анализа подозрительного программного обеспечения.

Для динамического анализа существуют следующие средства:

«DroidBox» – представляет собой автоматизированное средство динамического анализа для приложений Android. В результате анализа apk файла приложение позволяет определить и зафиксировать следующие события:

– операции с файловой системой;

– получение и отправку сетевых пакетов;

– запуск и установку служб в операционную систему;

– утечку пользовательских файлов и личной информации посредством сети «Интернет» и смс;

– попытки программы обойти существующие для нее ограничения и права;

– криптографические операции;

– отправка смс и выполнение телефонных звонков.

Кроме того, DroidBox генерирует графическую визуализацию поведения программы (цепочки событий) (рис. 2). Также при необходимости графическая визуализация позволяет наглядно оценить сходство поведения между анализируемыми программами.

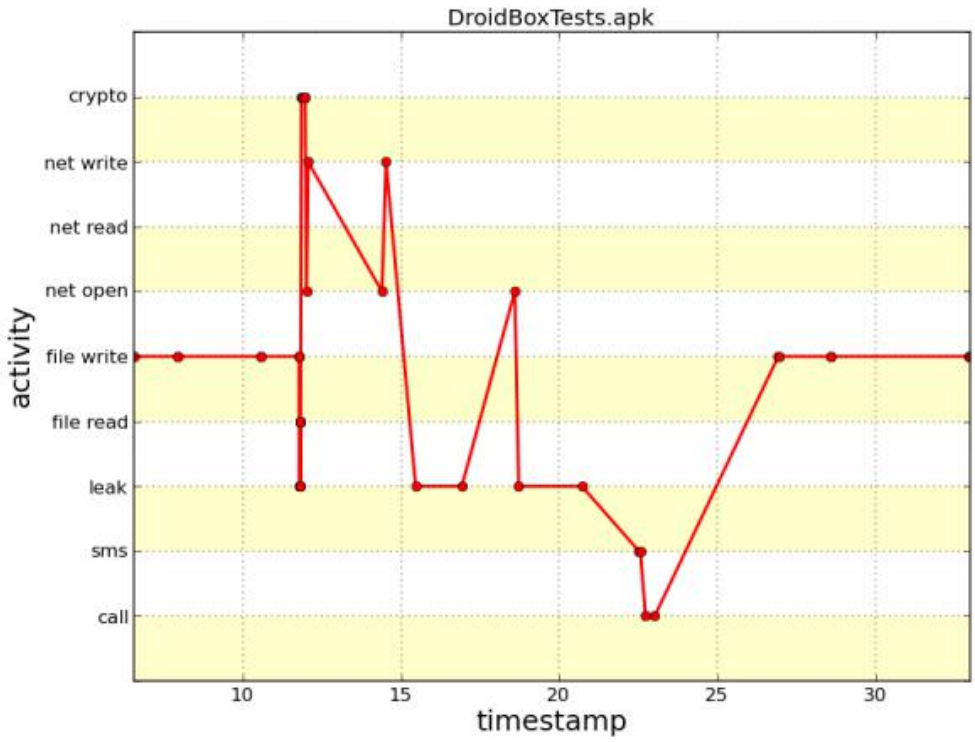


Рис. 2. Графическая визуализация процесса

Android SDK. Это комплект разработки программного обеспечения. Данное средство позволяет создать виртуальное Android устройство, и наблюдать за вредоносными программами в «безопасной среде».

AndroidAuditTools – дополнительный инструмент автоматизированного динамического анализа.

Средства статистического анализа: Mobile SandBox – веб-сервис, позволяющий выполнить анализ; IDA Pro – универсальный дизассемблер; APKInspector; Dex2jar; Androguard; Jd-gui.

Оптимальным способом применения существующих методов и средств исследования является комбинированное исследование путем статистического и динамического анализа приложения в «безопасной среде» с использованием, например, ADB интерфейса.

Библиографический список

1. https://yandex.ru/company/researches/2016/ya_search_2016, дата обращения: 12.10.2017.
2. https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/ дата обращения: 12.10.2017.
3. Akash Malhotra, Pawan Prakash Singh Android Malware: Study and analysis of malware for privacy leak in ad-hoc network // Journal of Computer Engineering. Jul.–Aug. 2013.
4. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.
5. Васильева Е. А., Пузарин А. В., Захаров Д. Н. Исследование возможности применения биллинговых записей // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 52–55.

Л. М. Трибунский [1]

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ДАННЫХ В МНОГОФАКТОРНОМ АНАЛИЗЕ СЛОЖНЫХ СИСТЕМ

Цифровизация в планировании многофакторных экспериментов. Человек сталкивается с огромным количеством проблем, которые ему приходится решать. Лучше всего, если способы решения проблем он получил в процессе воспитания и образования, а если нет, то необходимо создать систему, позволяющую решать возникающие задачи. Уровень развития науки и техники позволят это сделать.

Реальный мир нам дан в ощущениях. Для решения мы можем перевести задачу в виртуальный мир – мир математики и логики.

Цифровизация – это перевод заданной системы в вид понятный для универсальной обработки вычислительной техникой. Пока не пришел настоящий, искусственный интеллект, переводятся не только предме-

[1] Старший научный сотрудник Института металлургии имени А. А. Байкова РАН кандидат технических наук. © Трибунский Л. М., 2018.

ты (оцифровывание), но и правила действия. Мы получаем виртуальный объект и алгоритм использования его для наших целей.

Прикладная математика создавалась для обслуживания технических (естественных) и гуманитарных наук. Развитие вычислительной техники и программного обеспечения привело к цифровой эпохе. Настало время перевода естественно-научных знаний в области общественной жизни. Эксперимент (наблюдение) может использоваться везде, где требуется качественная информация. Самое лучшее – это мысленные эксперименты, основанные на глубоком знании предмета.

Прикладная математика падчерица, а планирование эксперимента сирота. В 50-х годах XX столетия было создано планирование многофакторного эксперимента на малом количестве уровней и это было ошибкой. Факторов в исследовании может быть 10 и больше, но это не решаемая проблема для принятых систем. Планирование должно быть рассчитано на любое количество факторов. Каждый новый фактор требует два или три дополнительных опыта, рабочая матрица получается нечетной и размерностью не менее девяти. План исследования есть основа положительного результата. Известные способы планирования громоздки (большое количество опытов) и дают плохую математическую модель исследуемой системы, что губит исследование.

Для решения сложной проблемы должна быть связь: правильная постановка задачи, путь ее решения, намечаемый результат и путь его получения и использования. Планирование эксперимента на основе матриц применялось в исследованиях автора с 1975 г. Все планы были построены по системе минимального коэффициента корреляции между отдельными факторами. Матрица 3x3 представлялась мало интересной. Рациональные матрицы – нечетные, например 5x5, хотя легко построить любую. Принцип – волновой плюс полволны.

Проводить по одному опыту на каждом уровне это хорошо, но слишком мало, поскольку между столбцами существует сильная корреляция. Необходимо провести серию опытов, максимально поменяв экспериментальные точки в пространстве.

С полученными экспериментальными данными можно работать как с простыми однофакторными экспериментами (при средних остальных). Для экспериментального исследования необходима точность в центре плана [1, 2].

Экспериментальное исследование является основным видом познания природы. Если реальный эксперимент поставлен быть не может, то требуется наблюдение или численный эксперимент.

Матрица плана девять факторов на девяти уровнях

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
1	2	3	4	5	6	7	8	9
2	4	6	8	9	7	5	3	1
3	6	9	7	4	1	2	5	8
4	8	7	3	1	5	9	6	2
5	9	4	1	6	8	3	2	7
6	7	1	5	8	2	4	9	3
7	5	2	9	3	4	8	1	6
8	3	5	6	2	9	1	7	4
9	1	8	2	7	3	6	4	5
5	5	5	5	5	5	5	5	5

Результаты проведенных исследований могут быть представлены в виде таблицы. Полученные значения каких-то свойств – это функции. Переменные, при которых они получены, рассматриваются как факторы. Другими словами, факторы – это причины, следствие – это функции. Факторы бывают управляемые (мы их задаем и поддерживаем) и не управляемые, мы их фиксируем (записываем).

Если в системе существует причинно-следственная связь, то результаты эксперимента могут быть представлены в виде математической модели. На первом этапе аппроксимация – это алгебраическое выражение, которое впоследствии может привести к созданию теории. Такая модель дает возможность вычислять значения функции при подстановке численных значений тех или иных факторов (параметры системы).

Методология построения математических моделей на основе многофакторных экспериментов. Методология экспериментального исследования включает разработку плана, реализацию плана, моделирование, проверку адекватности модели и интерпретацию результатов.

В качестве оптимизации процесса может использоваться «метод Гаусса – Зейделя», где процесс задается постепенным закреплением всех факторов, кроме одного, и так до конца. Если принят план многофакторный, то в классическом варианте это «крутое восхождение» по «Уилсону – Боксу».

В качестве объекта исследования может быть выбрана любая система. Для рассуждений примем математический подход к исследованию физических и химических явлений (процессов). Начнем с опреде-

лений. Объект исследования – это совокупности физических тел. Предмет исследования – это влияние воздействий на тела. Предмет воздействия будем называть фактором. Реакция объекта на воздействие является функцией отклика, т. е. собственно результатом, полученным после воздействия.

В качестве оболочки (математического обеспечения) был выбран МАТКАД-15, который весьма удобен не только для вычисления, но и оформления работ, связанных с моделированием сложных систем.

Для отработки методологии планирования эксперимента была выбрана матрица 11х11. Принцип построения плана – минимальная линейная связь между столбцами, числа в которых являются уровнями значений факторов. Строка определяет значение уровней для каждого из факторов. В такой схеме можно проводить исследование одиннадцатифакторной системы, что во многих случаях достаточно.

Не имя возможности ставить сложные эксперименты, автор пошел путем Пойи. Мы знаем ответ задачи и доказываем, что выбранным способом задача решается. Для начала, чтобы показать возможность методологии системы, была выбрана такая система, которая теоретически не может быть смоделирована даже при неразумно большом количестве уравнений, но за счет наглядного представления позволяет составить о себе достаточно цельное представление.

На первом этапе нас интересует только план исследования. Исследуемая система является произведением девяти функций, которые являются факторами (один из факторов прямая линия). Факторы – не математические кривые, т. е. их очень трудно описать уравнениями. Мы показываем плодотворность плана, который требует минимальной связи между столбцами. Заметим, что применение случайных чисел – это путь в никуда. Случайные числа не подходят для планирования многофакторных экспериментов.

Матрица для планирования эксперимента (дизайн для эксперимента) построена по «волновому» принципу. Первый столбец – полволны, от единицы до 11, второй столбец от двух до одного через 11 (две пол волны). Третий столбец – три пол волны от трех до одиннадцати, а затем через единицу до десяти и так далее. Такая «упорядоченная» матрица всего одна из общего числа 11 в 11 степени вариантов. По теории, для такого плана требуется ортогональность и ротатабельность, но мы их обойдем, взяв в качестве второй половины серии матрицу зеркальную первой. Проведя 12 прогонов (первый средний для всех факторов,

остальные по плану первой половины серии экспериментов), мы уже получаем некоторое представление об исследуемой системе.

Вторая половина серии (еще 12 прогонов) практически ставит точки над «И». Во многих случаях исследование на этом закончено. По принципу «черного ящика» строим математическую модель многофакторного эксперимента, а по ней выбираем нужные нам результаты.

Первая проверка состоит в построении модели в предположении, что мы проводили однофакторные эксперименты со значительными ошибками. На следующем этапе для подтверждения правильности модели тасуем (переставляем) столбцы.

Существенно то, что рассматривается система, как N-мерное пространство, где все факторы перпендикулярны функции, и мы строим графики фактор – функция.

В результате мы получаем наглядное представление о влиянии каждого фактора, строим модели для первой и второй серий и сравниваем полученные многофакторные модели. Многофакторные модели можно строить, используя не все факторы и строить однофакторные из многофакторной системы.

Но математика дама строгая и требует доказательств, в математике для доказательств используют много критериев, упомянем два – Стъюдента и Кохрена, но они созданы для однофакторных и расширены для много факторных экспериментов. Доказывать будем на основе прогонов псевдо экспериментов по глобальному принципу, получив одинаковые результаты в двух сериях.

Для второй серии прогонов возьмем те же столбцы, но поменяем их местами, т. е. другое сочетание проводимых экспериментов. Если сочетаем обе системы (45 прогонов), то картина многофакторная ухудшится, но улучшается, если рассматриваем систему однофакторной.

Можно сравнивать первую и вторую серии по проекциям – они всегда схожи, но сильно отличаются по абсолютным значениям. Если выбрать правильные функции для моделирования и высокую точность всего, то получим идентичные модели с (невероятной) одинаковостью. Одинаковый результат из разных наборов экспериментов (23 эксперимента) означает, что работа закончена.

В математическом моделировании простых подходов не существует. Не может быть единой системы моделирования – аппроксимации экспериментальных данных. Алгебраические выражения всегда являются моделями. Использовались три способа моделирования много-

факторных экспериментов: через произведение по корреляции (произведение полином); последовательный подбор коэффициентов; разложение по функциям.

Математическое моделирование – это подбор уравнения для адекватного описания исследуемой системы. Правильная модель, в идеале, описывает систему во всех диапазонах выбранных факторов. Но мы выбираем в общем виде только положительные значения, при необходимости «нормализуем». Автор моделировал по экспериментальным данным прессование и спекание, восстановление различных хлоридов, обогащение угля и оптимизировал свойства сплава по составу и т. д.

Планировать эксперименты надо на 9–11 уровнях. В качестве математических моделей должны быть функции: экспоненциальные, логарифмические и степенные. Модель должна быть проверена независимыми экспериментами. Логическая информация – основа моделирования. Словесная информация должна ранжироваться, т. е. переводиться в числовой вид. Основа моделирования – причинно-следственные связи. Ложные связи не логичны. В сложных системах не бывает простых моделей. В науке столько науки, сколько адекватных математических моделей. Теория создается на основе эксперимента.

Представленные матрицы могут использоваться для передачи информации в сокращенном и зашифрованном виде. Подобрать и определить вид матрицы, на основе которой передается информация как графическая, так числовая и смысловая, не представляется возможным даже для самых быстро действующих машин. Расшифровать можно только при условии знания всех параметров процесса шифровки.

Другой аспект – переработка информации для сравнения с уже имеющейся, например, сравнение части информации с базой данных для выявления деталей.

Многофакторные системы при выборочном обследовании почти всегда приводят к неправильным выводам. Разные выборки дают разный результат. Увеличение точности может происходить только при выборе правильной матрицы обследования. Репрезентативная выборка – не число, а подход к выбору от частей целого.

Библиографический список

1. Саутин С. Н. Планирование эксперимента в химии и химической технологии. – М. : ХИМИЯ, 1975.

2. Батунер Л. М., Позин М. Е. Математические методы в химической технике. – М. : ГХИ, 1960.

М. Б. Кавешников [1]

О ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Со времен Алана Тьюринга применяется теоретический прием, когда решение сложной математической или вычислительной задачи представлялось в виде абстрактных вычислительных машин. Впоследствии на их основе формулировались вполне реализуемые технические подходы и создавались действующие компьютерные системы. Так, попытки объяснить работу человеческого мозга привели к разработке искусственных нейронных сетей и появлению понятия искусственный нейрон [1]. Им является простейший аналоговый элемент, который моделирует работу нейрона биологического (рис. 1).

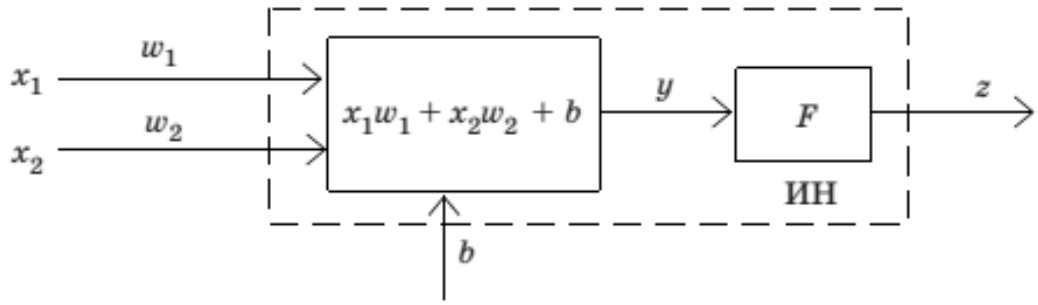


Рис. 1. Искусственный нейрон

x_1 и x_2 – входные сигналы, ω_1 и ω_2 – веса входных сигналов, b – смещение, y – взвешенная сумма или произведение вектора весов на входной вектор, F – функция активации, z –выход искусственного нейрона.

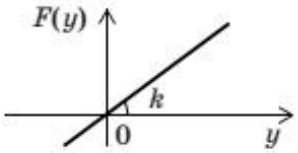
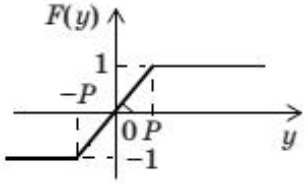
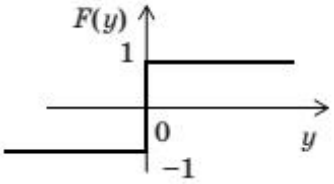
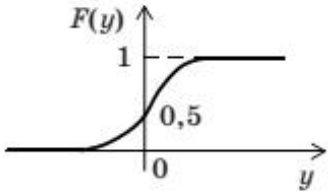
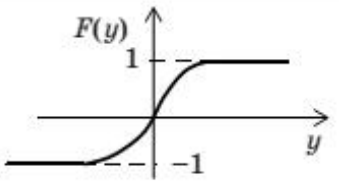
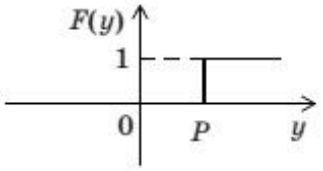
На вход искусственного нейрона поступает сигнал, он умножается на вес и суммируется со взвешенными сигналами с других входов. Получив сигналы с других нейронов, нейрон возбуждается и подает сигнал на выход. Этот процесс описывается активационной функцией. Ею может быть простая пороговая функция, однако для того чтобы иметь возможность обучать сеть путем обратного распространения ошибки, в качестве активационной функции следует использовать функцию без скачков и разрывов [5]. Поэтому применяются функции типа сигмоида и др. Ниже в таблице приведены наиболее часто встречаемые функции активации нейрона [1].

---

[1] Кандидат технических наук, доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя.
© Кавешников М. Б., 2018.

Таблица

Основные варианты описания активационной функции

Название функции	Описание	Графическое представление
Линейная	$F(y) = ky$, $k > 0$, k – коэффициент активации	
Линейная с насыщением	$F(y) = \begin{cases} +1, & y > P, \\ ky, & \lvert y \rvert < 1, \\ -1, & y < -P \end{cases}$	
Определение знака	$F(y) = \operatorname{sgn}(y)$	
Униполярная сигмоидальная (s-образная)	$F(y) = \dfrac{1}{1+\exp(-ky)}$, $k > 0$	
Биполярная сигмоидальная (гиперболический тангенс)	$F(y) = \operatorname{th}(ky)$, $k > 0$	
Пороговая	$F(y) = \begin{cases} 1, & y \geq P, \\ 0, & y < P \end{cases}$	

Имеется геометрическая интерпретация простых нейронных сетей. Один нейрон с одним входом фиксирует превышение сигнала заданной величины. Нейрон с двумя входами разбивает плоскость на две половины и показывает, в какой из них лежит точка, задаваемая координатами x_1 и x_2, а граница имеет уравнение $\omega_1 \cdot x_1 + \omega_2 \cdot x_2 + b = 0$ (рис. 2).

Попадание точки в полосу между двумя прямыми: $\omega_1 \cdot x_1 + \omega_2 \cdot x_2 + b = 0$, и $\omega_3 \cdot x_1 + \omega_4 \cdot x_2 + b_1 = 0$

Ширина полосы может быть определена, как $H = \left|(b - b_1) \cdot \frac{\omega_2}{\omega_1}\right|$

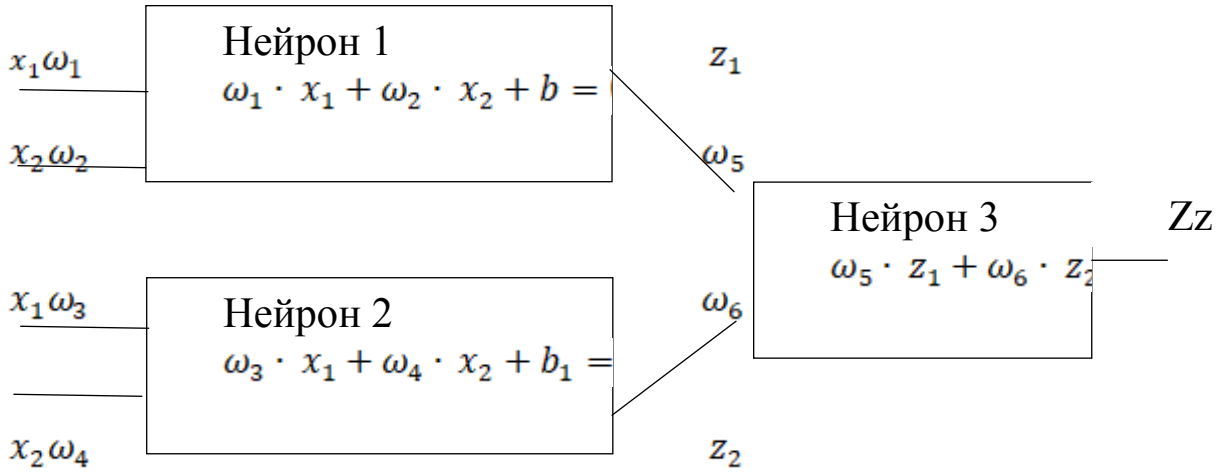


Рис. 2. Сеть из трех нейронов,
определяющая попадание точки в заданную полосу

Активатизационная функция может быть простейшей пороговой функцией:

$$Z_1 = \begin{cases} 1, \text{если } \omega_1 \cdot x_1 + \omega_2 \cdot x_2 + b \geq 0 \\ 0, \text{если } \omega_1 \cdot x_1 + \omega_2 \cdot x_2 + b < 0 \end{cases}$$

$$Z_2 = \begin{cases} 1, \text{если } \omega_3 \cdot x_1 + \omega_4 \cdot x_2 + b_1 \geq 0 \\ 0, \text{если } \omega_3 \cdot x_1 + \omega_4 \cdot x_2 + b_1 < 0 \end{cases}$$

$$Z_z = \begin{cases} 1, \text{если } \omega_5 \cdot z_1 + \omega_6 \cdot z_2 + b_2 \geq 0 \\ 0, \text{если } \omega_5 \cdot z_1 + \omega_6 \cdot z_2 + b_2 < 0 \end{cases}$$

Для того, чтобы эта нейронная сеть определяла попадание точки с координатами x_1 и x_2 в полосу определяемую двумя параллельными прямыми, необходимо найти значения весов ω_i (i=1, 2, …6) и смещений $b, b_1\, b_2$. При этом из геометрических условий можем получить соотношения:

$\omega_1 = -\omega_3$, $\omega_2 = -\omega_4$, $H = \left|(b - b_1) \cdot \frac{\omega_2}{\omega_1}\right|$, $\omega_5 = \omega_6 = 1$, $b_2 = -1$.

Из этого следует, что для определения весов и смещений достаточно определить уравнение первой прямой $\omega_1 \cdot x_1 + \omega_2 \cdot x_2 + b = 0$, определив величины ω_1 ω_2 b, и задав ширину полосы H. Однако есть другой способ получение весов и смещений – на основе некоторого контрольного множества точек с парами координат x_1 и x_2. Такое решение носит адаптивный характер и называется обучением нейронной сети. Суть этого подхода заключается в том, что рассчитывается множество точек, для которого факт попадания в полосу известен точно. Для какого-то начального множества весов и смещений вы-

числяются выходы Zz нейронной сети и сравниваются с эталонными значениями. Отличия выходов от их правильных значений по принципу обратной связи используют для корректировки предварительно выбранного множества весов и смещений.

Практически, если нейронную сеть на рис. 3 применить дважды к двум пересекающимся полосам, и их выходы проанализировать новым нейроном, объединяющим эти сети, то объединенная сеть будет способна определять факт попадания точки в прямоугольник или ромб.

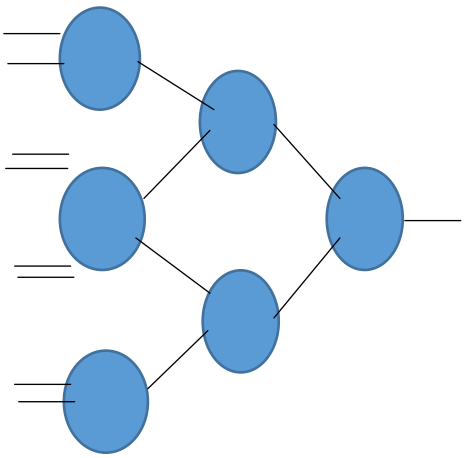


Рис. 3. Сеть из нейронов с двумя выходами, позволяющая определять попадание точки в прямоугольник или ромб

Приведенные выше примеры интересны тем, что имеют геометрическую интерпретацию и помимо традиционного метода обучения множество весов и смещений можно определить по формулам аналитической геометрии [2]. Увеличивая число нейронов, можно определять попадание точки в сложные полигоны. Рассматривая много входов, мы рассматриваем многомерное пространство и задачи сложной многокритериальной классификации. Преимущества нейронных сетей перед другими математическими подходами заключаются в следующем [3, 7]:

В возможности представления в виде нейронной сети сложных и трудноформализуемых алгоритмов и математических решений.

В возможности представления решения для реализации на параллельных вычислительных системах.

В едином методическом подходе к решению задач классификации, распознавания образов, аппроксимации, моделирования, а также в альтернативных подходах к решениям, которые могут быть получены традиционными методами [6, 8].

Можно выделить основные направления в области компьютерной безопасности, где применяются нейронные сети:

Идентификация пользователя по биометрическим данным.

Обнаружение вредных процессов на основе анализа состояния компьютера и компьютерной сети. Защита от вирусов, руткитов, троянских коней, проникновений в систему.

Выявление уязвимостей и управление рисками информационной безопасности.

Одним из недостатков подхода с использованием нейронных сетей – трудноформализуемые алгоритмы выполняющие сложные вычисления практически невозможно верифицировать, и сами алгоритмы не гарантируют правильности полученных решений. Доказывать надежность и правильность полученных результатов приходится на экспериментальных данных.

Библиографический список

1. Бураков М. В. Нейронные сети и нейроконтроллеры : учеб. пособие. – СПб. : ГУАП, 2013. – 284 с.

2. Цыпкин А. Г., Цыпкин Г. Г. Математические формулы. Алгебра. Геометрия. Математический анализ : справочник. – М. : Наука. гл. ред. физ.-мат. лит- ры, 1985. – 128с.

3. Спицын В. Г., Цой Ю. Р. Применение искусственных нейронных сетей для обработки информации: методические указания к лабораторным работам. – Томск : Изд-во ТПУ, 2007. – 31 с.

4. Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. – 2011. – № 3 (7). – С. 3–15.

Раздел 5. РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ

А. Г. Власюк[1], *В. В. Гончар*[2]

ИСПОЛЬЗОВАНИЕ СЛЕДОВАТЕЛЕМ СОВРЕМЕННЫХ ЗНАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации» информация – это сведения (сообщения, данные) независимо от формы их представления.

Современное законодательство направлено на использование достижений науки и техники.

В соответствии со ст. 11 Федерального закона «О полиции» полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

Одним из наиболее значимых знаний в области расследования преступлений, связанных с компьютерной информацией выступают достижения науки Форензики [1, с. 12–15]. Прикладные знания из выработанных Форензикой методов экспертного исследования компьютерной информации позволяют следователю преобразовать их в умения, необходимые при расследовании преступлений информационной направленности. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [2, с. 44]. Проведение комплекса следственных действий в условиях недостаточных знаний современных информационных технологий делает затруднительным сохранение, интерпретацию компьютерных данных [7].

Расследование преступлений информационной направленности состоит в сборе, фиксации, проверке и оценке доказательств, связанных с информационными технологиями.

---

[1] Курсант 4 В курса Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Власюк А. Г., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

Основная цель при проведении таких работ – использование методов и средств для сохранения (неизменности), сбора и анализа цифровых вещественных доказательств, для того чтобы восстановить обстоятельства совершения преступления.

Наиболее распространенным средством доказывания является информация на электронных носителях информации. Знания в области информационных технологий определяют профессионализм и компетентность следователя. Обеспечения следователем порядка получения сведений согласно требованиям законодательства должно соответствовать признаку допустимости. Здесь важное значение имеет правильное копирование информации, ее выемки с обязательной фиксацией в протоколе ее особенностей. Здесь знания в области информационных технологий играют ключевую роль.

Одно лишь выключение компьютера ведет к утрате сведений из оперативной памяти, где фиксируются проводимые пользователем операции во время своей работы. В программах связи и работы с сетью сохраняются данные о контактах пользователя. Реестр системы хранит сведения о типах документов, информация о свойствах папок, установленном оборудовании и установленных портах. Этап осмотра включает в себя упаковку носителя информации. Все действия должны соответствовать определенным гостам. Это не новелла, «ГОСТ 6.10.4-84. Государственный стандарт Союза ССР. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения».

Глобальная компьютерная сеть и развитие облачных технологий нивелирует изъятие аппаратных средств на территории Российской Федерации. Одним из реквизитов электронного документа выступает электронная цифровая подпись [2, с. 47]. Она защищает документ от преобразования путем применения алгоритмов криптографии, позволяя идентифицировать пользователя через путь сертификатов, первичным из которых является удостоверяющий центр. Проблема уничтожения или искажения компьютерной информации может быть решена повышением уровня знаний в вопросах использования компьютерной информации следователя.

Совершаемые посредством сети «Интернет» преступления могут совершаться с помощью аппаратных средств, принадлежащих другим лицам. Это становится возможно при помощи вредоносных компьютерных программ, предоставляющих доступ к управлению компьютером. Осо-

бая сложность состоит в том, что преступники применяют программное обеспечение, которое, не получив в установленное время подтверждение, удаляет информацию. Как правило, следователи обращают внимания на аппаратные средства, принятые называть «персональным компьютером», «ноутбуком», однако в настоящее время «смартфон» имеет технические характеристики, не уступающие стационарным аппаратным средствам. Многие технологические компании в рамках развития разрабатывает устройства, позволяющие приспосабливать «смартфон» под десктопное устройство. Имеет место ознакомиться следователю с методическими рекомендациями по проведению компьютерно-технической экспертизы. Осведомленность следователя в современных информационных технологиях помогает решить проблему назначения компьютерной или радиотехнической экспертизы при исследовании протоколов wi-fi. Обозначим также, что знания не ограничиваются техническими свойствами и принципами работы тех или иных технических средств. Ввиду быстрого развития информационных технологий одно из ведущих направлений – это автоматизация сбора данных и их обратное представление. В данном случае будет верным воспринимать информационные технологии в качестве виртуального консультанта. В случае расследования преступлений информационной направленности применение знаний в информационных технологиях позволяет оптимизировать организацию расследования, разработки и внедрения плана по расследованию, описание наиболее вероятных механизмов и сценариев атаки, а именно:

– установление факта неправомерного доступа к информации в компьютерной системе или сети;

– установление места несанкционированного проникновения в компьютерную систему или сеть;

– установление времени совершения преступления;

– установление надежности средств защиты компьютерной информации;

– установление способа несанкционированного доступа;

установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления;

– сбор доказательной базы;

– выявление обстоятельств, способствовавших преступлению;

– установление вредных последствий преступления;

– основная сфера применения знаний информационных технологий – расследование преступлений, в которых фигурирует компьютерная ин-

формация как объект посягательства, электронно-вычислительная техника как орудие совершения преступления, а также цифровые доказательства преступления [6].

Рассмотрим некоторые из программ, которые могут оказать содействие следователю: помощник в работе с RAM (оперативной памятью) может выступить программа «KeeFarce» – извлечение паролей KeePass из памяти; Wireshark – известнейший сетевой сниффер; FastIR Collector – обширный сборщик информации о системе Windows (реестр, файловая система, сервисы, автозагрузка и т.д.); chrome-url-dumper – извлечение информации из Google Chrome; hindsight – анализ истории Google Chrome/Chromium; CyberChef – мультиинструмент для декодирования данных.

При осмотре рабочего стола аппаратного устройства полезным будет отразить наличие специализированных утилит, предполагающих их использование в преступной деятельности. Примерами могут служить следующие утилиты: Reaver – утилита для подбора PIN-кода для WPA беспроводных сетей; Nmap – сканер уязвимостей; Aircracking – набор утилит для пентеста беспроводных сетей.

Средства пентеста: ManageEngine Security Manager Plus; GFI LANguard Network Security Scanner; Security Database Website.

Эти программы показательны и носят информативный характер, их наличие и использование способствуют построению модели преступника:

– способен ли самостоятельно изучить и применять методы пентеста, используя специализированные сайты и программное обеспечение, так называемые «головоломки для хакеров» – среда для обучения пентесту;

– способен ли он самостоятельно освоить стандарт выполнения тестов на проникновение (Penetration Testing Execution Standard – PTES), разрабатываемого сообществом пентестеров.

Специфический характер преступлений в области информационных технологий предполагает определенный подход к определению обстоятельств, подлежащих доказыванию, а именно: время и место проведения атаки; используемые для подготовки и проведения инструменты; приобретение demo/trial средств взлома; изучение работы приобретенного средства пентеста; выбор объекта атаки; сетевое сканирование объекта атаки, которая проводится в форме запросов DNS, сканирования портов, эхо-тестирования; использования каталога CVE для интерпретации результатов сканирования.

Для проведения работ по сбору цифровых доказательств необходимо придерживаться принципов неизменности, целостности, полноты информации и ее надежности. При проведении следственного действия – допрос с подозреваемым по делам о преступлениях информационной направленности, важно показать себя как минимум осведомленным в области информационных технологий, т. к. зачастую «киберпреступники» используют в обороте аббревиатуры, понятия и определения технического характера [5].

Корпоративная сеть: веб-сайт компании; почтовый сервис; CRM-систему; AD; АРМ на базе Win7/Win10; вспомогательные сервера и службы; АРМ и сервисы технического персонала; защитные средства.

Вектора атак: OWASP TOP-10; MiTM; Public vulns; Security policy vulns; Privilege escalation; обход защитных средств; misconfiguration.

Знания в области информационных технологий дают представления о наиболее часто встречающихся сценариях кибератак внутри сети и на аппаратные средства. Примером может служить следующий сценарий:

Исследование периметра компании, обнаружение уязвимости и обеспечение себе точки входа в корпоративную сеть. Используя атакованные ранее машины как плацдарм продвигаться по сети, выявляя новые цели для атаки, пока не будет получен контроль над всеми машинами в сети.

Методологические рекомендации по выработке знаний в области информационных технологий.

Применение этих знаний в следственных действиях и иных мероприятиях на этапах предварительного расследования [3, с.14].

Уяснение специализированной терминологии и моделей взлома информационных систем.

Эти обстоятельства определяют актуальность темы исследования.

Цель работы – указать на необходимость усвоения знаний в сфере информационных технологий при расследовании преступлений информационной направленности как важного инструмента профессионализма следователя. Продемонстрировать вспомогательную функцию данных знаний, имеющих практический уклон в рамках проведения следственных действий. Выработать рекомендации по организации расследования с учетом особенностей преступлений в сфере информации.

Для уяснения основных понятий необходимо обратиться к нормативным документам и разъяснительным рекомендациям, определяющим правовые отношения в области информационных технологий:

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;

Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;

Справочная информация: «Профессиональные стандарты» (Материал подготовлен специалистами КонсультантПлюс;

http://www.rkn.gov.ru/ «Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty «Федеральная служба по техническому и экспортному контролю (ФСТЭК России)» [4, с.134].

Библиографический список

1. Федотов Н. Н. Форензика – компьютерная криминалистика. – М. : Юридический мир, 2007. – 432 с.

2. Галатенко В. А. Основы информационной безопасности [Электронный ресурс]. – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266с.

3. Гончар В. В., Мешков М. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования // Мировой судья. – 2015. – № 4.

4. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

5. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.

6. Васильева Е. А., Пузарин А. В., Захаров Д. Н. Исследование возможности применения биллинговых записей // Технологии информационной безопасности в деятельности ОВД : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 52–55.

7. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (том 2).

Е. Ю. Самолаева[1]

ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Повышение качества расследования уголовных дел о совершении преступлений в сфере компьютерных технологий в настоящее время приобрело особое значение. На фоне растущего числа преступлений, совершаемых в сфере компьютерной информации (в 2017 г. на 7,7 % больше зарегистрировано, чем в 2016 г.), а также увеличивающегося числа преступлений, совершаемых с использованием компьютерных технологий, раскрываемость их существенно снижается (так, почти на 20 % меньше раскрыто преступлений в сфере компьютерной информации в 2017 г., чем в 2016 г.) [1]. Таким образом, вопросы организации расследования преступлений данной категории требуют тщательного исследования в целях выявления причин такого снижения. Также во многих случаях уголовные дела о преступлениях, связанных с использованием компьютерных технологий не возбуждаются в связи со сложностью их квалификации и малочисленной практикой их расследования.

Преступления, совершенные с использованием компьютерных технологий, в основном возбуждаются на основании материалов оперативно-разыскной деятельности. Также положительный результат в области раскрытия подобных преступлений связан с правильной организацией взаимодействия с другими подразделениями и службами правоохранительных органов. Наиболее перспективные для расследования и дальнейшего направления в суд материалы связаны с задержанием лиц, совершавших данные преступление, в ходе реализации оперативной разработки. После задержания следователю необходимо выполнить алгоритм действий, включающий следственные и процессуальные действия: составление протокола задержания; производство выемки предметов, которые могут использоваться для хранения, уничтожения, блокирования, модификации или копирования компьютерной информации (флеш-накопители, мобильные телефоны, портативные компьютеры); осмотры с участием специалистов изъятых предметов; обыски; направления органу дознания отдельных поручений о производстве следственных, оперативно-разыскных действий, направленных на выявление связей подозреваемого, установлению ис-

[1] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Самолаева Е. Ю. 2018.

точников приобретения им имущества; допрос свидетелей; получение образцов для сравнительного исследования; назначение судебных экспертиз (судебные компьютерные экспертизы, фоноскопические, почерковедческие и др. судебные криминалистические экспертизы) и т. д.

Расследование преступлений, совершаемых с использованием компьютерных технологий, предполагает деятельность следователя по сбору доказательств (ст. 86 УПК РФ) в рамках предмета доказывания (ст. 73 УПК РФ). Однако, несмотря на урегулирование УПК РФ данных вопросов, правоприменительная практика складывается не единообразно.

Так, в ходе расследования преступлений с использованием компьютерных технологий сложности могут возникнуть с установлением времени и места совершения преступления. По данным следственной практики, временные атрибуты файла часто подвергаются фальсификации (посредством перевода часов вперед или назад или их остановки с использованием специальных программ) [2, с. 46-51]. Такого рода действия затрудняют оценку достоверности сведений, содержащихся в файле документа, и не позволяет его использовать в качестве доказательства. Сложнее устанавливать место совершения преступления в связи с тем, что в данных преступлениях им может признаваться не только традиционный его вид (физический адрес), но и часть информационного пространства (домен, сайт), в котором фактически было совершено преступление активным пользователем. Например, это сайт, который зарегистрирован на сервере, имеющем физическое местоположение, и лицо, его пользователь, находившийся в момент совершения преступления по конкретному адресу [3, с. 199–203].

Также сложности в доказывании представляют использование доказательств в электронной форме. Текущие требования, предъявляемые к электронным носителям информации, состоят в том, что они должны быть в оригинальном, а не скопированном виде (п. 5 ч. 2 ст. 82, ч. 9.1 ст. 182 УПК РФ). В то же время позиция высших органов власти по данному вопросу – запретить следственным органам изымать серверы и жесткие диски при проведении следственных мероприятий (правда, на предприятиях, чтобы не приостанавливалась их деятельность) [4].

Осмотр электронного носителя информации трудоемок. Количество файлов на носителе может быть большим. Поскольку не известно изначально, какой файл может быть значим для расследования, фик-

сации информации, находящейся на носителе, обычно занимает достаточно много времени [5, с. 48–51].

Использование специальных познаний в сфере компьютерных технологий также занимает неотъемлемую часть расследования [9]. Успех расследования напрямую зависит от тесного взаимодействия со специалистами и своевременного назначения судебной компьютерной экспертизы. Следователь должен знать объект исследования данной экспертизы, ее разновидности, вопросы, которые можно поставить перед экспертом. Так, в науке приводится следующая разновидность компьютерных экспертиз: судебная аппаратно-компьютерная, судебная компьютерно-программная, судебная информационно-компьютерная экспертиза, судебная компьютерно-сетевая экспертиза [6, с. 109–113]. На практике назначается в основном компьютерно-техническая [7].

В некоторых случаях следователь может принять решение не назначать экспертизу, а получить показания от специалиста, в частности провести осмотр объекта с его участием. Показания специалиста также могут быть положены в основу обвинения. Следователю только необходимо правильно определить, в каком случае это целесообразнее сделать. Данный вопрос рассматривается в юридической литературе неоднозначно. Основная проблема заключается в содержании экспертизы (как исследования в целях решения поставленных вопросов) и осмотра (позволяющего обнаружить и зафиксировать компьютерную информацию) [8, с. 129–132]. Не вызывает сомнения только тот факт, что при проведении данных следственных действий участие специалиста (эксперта) необходимо.

Знание правил работы с компьютерной информацией, позволяющее не допустить возможность ее потери, также является одним из важных условий успешного расследования преступлений, совершенных с использованием компьютерных технологий. Поэтому, если есть вероятность, что в ходе осмотра может быть уничтожена или повреждена информация, необходимо обязательно привлекать специалистов или назначить судебно-компьютерную экспертизу. В первую очередь это касается изучения неочевидных средств компьютерной техники и компьютерной информации (например, замаскированная сетевая карта) или необходимости разрешения идентификационных вопросов.

В заключение отметим, что, несмотря на принимаемые меры по совершенствованию законодательства в сфере доказывания, в рассматриваемой сфере много не разрешенных на практике и требующих обсуждения вопросов.

Библиографический список

1. Состояние преступности в России за январь-декабрь 2017 года. – МВД России ФКУ «ГИАЦ» [Электронный ресурс] : Режим доступа : URL: http:// www.mvd.ru.

2. Першин А. Н. Временные следы при расследовании преступлений, совершаемых с использованием компьютерных технологий // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2016. – № 1. – С. 46–51.

3. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. – 2017. – Т. 12. – № 5. – С. 199–203.

4. Путин запретил следователям изымать серверы и жесткие диски на предприятиях [Электронный ресурс] : Режим доступа : URL: http:// www.vesti.ru/doc.html?id=2917073&cid=7 (дата обращения: 5.02.2018).

5. Сидоров В. В., Новиков А. А. Особенности фиксации представленной информации в электронном виде криминалистически значимой информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2016. – № 2 (44). – С. 48–51.

6. Васюков В. Ф. Некоторые аспекты назначения судебной компьютерной экспертизы при расследовании хищений в сфере информационных и коммуникационных технологий // Вестник Удмуртского университета. Серия Экономика и право. – 2016. – Т. 26. – № 4. – С. 109–113.

7. Решение по делу 1-106/2016: Приговор Советского районного суда г. Тамбов (Тамбовская область) по обвинению С. Е. Полякова по ч. 2 ст. 273 УК РФ : [Электронный ресурс]: Режим доступа : URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tambova-tambovskaya-oblast-s/act-525703616.

8. Пропастин С. В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) // Современное право. – 2013. – № 6. – С. 129–132.

9. Городецкая Я. С., Гончар В. В., Захаров Д. Н. Некоторые проблемы расследования мошенничества в сфере компьютерной информации // Сборник научных трудов XV научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2017. – С. 91–96.

В. А. Саморока[1], ***М. Ю. Бекетов***[2], ***С. В. Гурдин***[3]

СПЕЦИФИКА ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ПОЗНАВАТЕЛЬНОЙ ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Рост информационных технологий в России обусловил расширение сфер применения электронных технологий, мобильных платежей в предпринимательской деятельности и в повседневной жизни. Стремительное развитие таких технологий создает предпосылки для их использования в преступных целях.

Одновременно с количеством пользователей данных электронных технологий растет число потенциальных жертв, а также возможность использовать сеть «Интернет» для совершения противоправных деяний. При этом анонимность глобальных информационных сетей и быстрота передачи информации позволяют использовать все эти преимущества для совершения преступлений, которые нередко именуются киберпреступлениями[4].

Такое состояние дел не может вызывать обеспокоенности со стороны высших должностных лиц государства. Именно по этой причине в Указе Президента Российской Федерации от 31.12.2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» в п. 22 обращается внимание на тот факт, что появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий.

Очевидно, что в таком случае борьба с этими видами противоправных явлений в современном обществе становится одним из приоритетных направлений деятельности правоохранительных органов, в особенности тех, которые осуществляют предварительное расследование по уголовным делам в отношении лиц, совершивших подобные преступления.

---

[1] Доцент кафедры уголовного процесса МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Саморока В. А., 2018.

[2] Доцент кафедры уголовного процесса МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Бекетов М. Ю., 2018.

[3] Доцент кафедры уголовного процесса МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Гурдин С. В., 2018.

[4] Понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве.

Специфика производства всех следственных действий при расследовании преступлений в сфере компьютерной информации в первую очередь проявляется в необходимости использования специальных знаний в различных отраслях науки и техники.

Как правило, это знания в области электроники, программирования, телекоммуникационных технологий и другие знания.

Следователь в большинстве случаев не обладает достаточными знаниями в указанных выше отраслях.

По этой причине возникает настоятельная необходимость привлечения к участию в производстве следственных и процессуальных действиях, особенно имеющих своим предназначением обнаружение, закрепление и изъятие информации в электронном виде или на электронном носителе, соответствующего специалиста.

Следует отметить, в данном случае это не просто необходимость, но и требование уголовно-процессуального законодательства, которое подлежит неукоснительному соблюдению.

Использование специальных знаний в познавательной процессуальной деятельности при расследовании преступлений, совершенных в сфере высоких технологий, осуществляется следователем в таких формах, как: консультации с соответствующим специалистом, который может дать пояснения о правилах обращения с вычислительной или компьютерной техникой, описать аппаратные устройства и программное обеспечение; оказание следователю содействия при производстве следственных действий в особенности тогда, когда его участие обязательно (например, при обыске или выемке электронных носителей информации), так он способствует поиску информации в компьютере; оказавшие помощи при изъятии средств вычислительной техники и информации, подготовке их к транспортировке и хранению; постановка вопросов эксперту при назначении экспертизы, а также участникам уголовного судопроизводства в целях их дальнейшего допроса.

В 2012 г. был внесен ряд изменений в нормативные правовые акты Российской Федерации, существенно расширивший потребности правоохранительных органов в специальных знаниях в области компьютерной информации в процессе выявления, раскрытия и расследования преступлений.

Так, Федеральным законом от 29.11.2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» ст. 82 УПК РФ, регла-

ментирующая процессуальный порядок хранения вещественных доказательств, была дополнена ч. 2.1 содержащей требование о необходимости привлечения специалиста для копирования содержащейся на электронных носителях информации на другие электронные носители информации, предоставленные законным владельцем изъятых электронных носителей информации или обладателем содержащейся на них информации, при этом при копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения.

Федеральным законом от 28.07.2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» ст.ст. 182 и 183 УПК РФ, регламентирующие основания и порядок производства обыска и выемки, дополнены ч. 9.1 и ч. 3.1 соответственно, в которых указывается на необходимость привлечения специалиста, если при производстве обыска (выемки) изымаются электронные носители информации. Если законный владелец изымаемых электронных носителей информации заявляет ходатайство об их копировании, то специалист, участвующий в обыске (выемки), в присутствии понятых осуществляет копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо по заявлению специалиста повлечь за собой утрату или изменение информации.

Изъятые в ходе следственного действия мобильные устройства, планшетные компьютеры, навигаторы и иные носители электронных следов упаковываются и опечатываются таким образом, чтобы обеспечить сохранность имеющейся в цифровой памяти информации. Для этого опечатываются все порты, слоты, входы и выходы электронного устройства, что удостоверяется подписями следователя, специалиста и понятых [1].

В то же время, по мнению В. В. Кальницкого, разумная идея исключить дополнительные негативные последствия (личного, коммерческого плана) от изъятия электронной документации вылилась в неоправданный запрет изъятия электронных носителей (например, флэш-карты) без участия специалиста, даже если при этом не производятся манипуляции с электронной техникой [2].

Также претерпела изменения ст. 15 (Права органов, осуществляющих оперативно-разыскную деятельность) Федерального закона от

12.08.1995 г. № 144-ФЗ «Об оперативно-разыскной деятельности». Федеральным законом от 29.11.2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» в данную статью был добавлен абзац, регламентирующий порядок изъятия документов и (или) электронные носители информации при проведении гласных оперативно-разыскных мероприятий.

Таким образом, у должностных лиц, осуществляющих оперативно-разыскную деятельность, предварительное расследование или судебное разбирательство возникают проблемы не только копирования информации по требованию законного владельца, изъятых электронных носителей информации или обладателя содержащейся на них информации, но и обеспечения для этого условий, исключающих возможность ее утраты или изменения, а также необходимости в большинстве случаев привлекать для этой процедуры соответствующего специалиста. Поскольку наибольшее доверие у правоохранительных органов заслуженно вызывают эксперты государственных судебных экспертных учреждений, наибольшая нагрузка по участию в осмотрах, обысках, выемках, копированию компьютерной информации легла именно на них.

При этом необходимо отметить, что, несмотря на постоянный количественный и качественный рост объектов, содержащих компьютерную информацию, широкое их использование при совершении преступлений, всевозрастающее количество изымаемой компьютерной техники, хоть сколько-нибудь сопоставимого роста численности экспертов государственных судебных экспертных учреждений и ведомств не происходит. Нагрузка по производству компьютерных экспертиз и исследований на протяжении последних лет превышает допустимую в разы. Резко увеличившаяся потребность в привлечении сотрудников экспертно-криминалистических подразделений к участию в осмотрах, обысках, выемках, иных следственных действиях и оперативно-разыскных мероприятиях приводит к сокращению их возможностей по исследованию уже изъятых и представленных на экспертизу объектов.

С учетом описанной проблемы важно оптимизировать работу по осмотрам, обыскам и выемкам компьютерной информации или устройств, содержащих информацию в электронном виде.

Как показывает практика, перед проведением таких следственных действий довольно часто не проводится никакой подготовительной

работы (в том числе оперативно-технических мероприятий) в целях установления местонахождения и функционального назначения средств вычислительной техники, наличия на них средств защиты информации и возможностей доступа к защищаемой информации; определения способов изъятия компьютерной информации (копирование на собственные машинные носители, изъятие только машинных носителей, изъятие машинных носителей вместе с содержащими их средствами вычислительной техники); выбора состава оборудования, необходимого для производства следственного действия; определения особенностей тактики проведения следственного действия (последовательность осмотра помещений и средств вычислительной техники в каждом помещении, необходимость привлечения персонала, необходимость осмотра на месте и порядок отключения средств вычислительной техники и компьютеров, если на момент проведения следственного действия они будут находиться во включенном состоянии и прочие).

Полагаем, что использование специальных знаний в познавательной процессуальной деятельности при расследовании преступлений, совершенных в сфере высоких технологий, есть обусловленная требованиями уголовно-процессуального законодательства и времени необходимость участия того или иного специалиста в производстве следственных или иных процессуальных действий для оказания содействия следователю и повышения таким образом качества всего предварительного расследования по таким уголовным делам в целом.

Библиографический список

1. Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. – 2014. – № 20. – С. 32.

2. Кальницкий В. В. Вопросы правовой регламентации следственных действий на современном этапе // Законы России: опыт, анализ, практика. – 2015. – № 2. – С. 34.

А. Ю. Петрунина[1], ***С. В. Ермаков***[2]

РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С каждым годом доля киберпреступлений в нашей стране увеличивается. По данным МВД России, в 2017 г. зафиксировано 9 058 преступлений, которые были совершены с использованием компьютерных технологий. 2016 г. в совокупности принес 66 тыс. таких преступлений, что в полтора раза превышает показатели 2015 г. (44 тыс.). Основной причиной увеличения числа киберпреступлений стал резкий рост мошенничеств (с 13,4 тыс. до 32,8 тыс. в год), а также краж (с 8,5 тыс. до 9,8 тыс.), совершенных путем использования Интернета и иных коммуникационных ресурсов. Существенно увеличилось и количество преступлений, связанных с хищением совершенных путем ввода, удаления, блокирования и модификации компьютерной информации (ст. 159.6 УК РФ) [1].

По данным статистики ФКУ «ГИАЦ МВД России» о состоянии преступности в 2017 г. раскрыто лишь 22,5 % зарегистрированных преступлений. За 2016 г. производство по уголовным делам о киберпреступлениях в 75 % случаев приостановлено за неустановлением лица [2], подлежащего привлечению к уголовной ответственности в качестве обвиняемого, примерно 6 % уголовных дел прекращено по реабилитирующим основаниям и только 7 % уголовных дел направлено с обвинительным заключением в суд. То есть количество совершаемых киберпреступлений – миллионы, а число осужденных по ним – всего лишь десятки [2].

С момента появления в Уголовном кодексе новых квалифицированных составов мошенничества, в том числе с использованием разнообразных карт для платежей и в сфере компьютерной информации (ст.ст. 159.1–159.6, 159.3 и 159.6) прошло пять лет, однако проведенный анализ судебной практики показывает, что, несмотря на появление в 2012 г. новых специальных видов мошенничества, единый подход к вопросам правоприменения и судебного толкования до сих пор отсутствует, в то время как имеющиеся пробелы в законодательстве ловко используются злоумышленниками.

---

[1] Курсант 421 учебного взвода Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Петрунина А. Ю., 2018.

[2] Заместитель начальника кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Ермаков С. В., 2018.

Несмотря на принятие постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [3], в настоящее время остаются дискуссионными следующие вопросы:

– Является ли уничтожением компьютерной информации деяние, при котором информация была изначально уничтожена, но через определенное время частично или полностью восстановлена специалистами?

– Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации?

– Можно ли квалифицировать написание программы компьютерного вируса на неэлектронном носителе (бумаге), как создание вредоносной компьютерной программы?

– Как можно квалифицировать действие преступника, направленное на неправомерное ознакомление с компьютерной информацией, когда у преступника есть возможность запомнить персональные данные лица, а затем воспроизвести их на другом материальном или электронном носителе?

– Применима ли к компьютерной информации категория собственности?

Особенность данной категории дел заключается в специальном предмете.

Предметом по ст. 159.6 УК РФ могут являться:

– компьютерная информация, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;

– имущество, т. е. все вещи лица, находящиеся в его собственности (включая деньги и ценные бумаги), а также имущественные права на получение вещей или имущественного удовлетворения от других лиц;

– информационно-телекоммуникационная сеть – совокупность технических средств для передачи и обработки информации [4].

Согласно ст. 159.6 УК РФ уголовно-наказуемыми будут лишь следующие способы совершения преступления:

1. Ввод компьютерной информации, т. е. размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения.

2. Удаление компьютерной информации, т. е. совершение действий, в результате которых становится невозможным восстановить со-

держание компьютерной информации, и (или) в результате которых уничтожаются носители компьютерной информации.

3. Блокирование компьютерной информации, т. е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерной информации, но не связанных с ее удалением.

4. Модификация компьютерной информации, т. е. совершение любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

5. Вмешательство в функционирование: средств хранения, средств обработки, средств передачи компьютерной информации, информационно-телекоммуникационные сети.

Раскроем некоторые понятия. Так, под вмешательством в функционирование следует понимать целенаправленное воздействие программных или программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, – или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации [5].

В качестве примера можно привести следующую ситуацию. 27 февраля 2016 г. приблизительно в 13 час. 45 мин. М. Г. Исмаилов в целях хищения чужого имущества, находясь у себя дома, с использованием персонального компьютера, подключенного к сети «Интернет» с принадлежащего Райханову О. Н. электронного счета в системе «Единый кошелек» путем перечисления на счет платежной системы «Киви-кошелек» за номером «89285485747» похитил денежные средства в сумме 5 тыс. 560 руб. 60 коп., после чего перечислил данную сумму на свой банковский счет в ОАО «Экспресс-банк» и обналичил посредством снятия через банкомат. Исмаилов М. Г. совершил мошенничество в сфере компьютерной информации, т. е. совершил преступление, предусмотренное ч. 2 ст. 159.6 УК РФ. Исмаилова М. Г. был признан виновным в совершении преступления, предусмотренного ч. 2 ст. 159.6 УК РФ, а также ему было назначено наказание в виде штрафа в размере 25 тыс. руб. в пользу государства [6].

Для успешного расследования данной категории преступлений необходимо проведение следователем (дознавателем) определенного комплекса следственных действий.

Самым первым и основным следственным действием, которое проводится во всех без исключения случаях, является осмотр места происшествия. Однако зачастую определить место, откуда было совершено преступление, бывает очень затруднительно [7]. Компьютерное мошенничество предусматривает наличие одного или нескольких устройств, которые используются (использовались) в процессе обмена информацией для извлечения информации. Однако между устройствами может быть огромное расстояние, от нескольких сотен метров до нескольких тысяч километров. Данная ситуация сильно замедляет процесс выявления, раскрытия и расследования мошенничества в сфере компьютерной информации, особенно когда получение информации осуществляется за границей.

Исходя из вышесказанного, местом совершения такого преступления будет именно местонахождение технических устройств, с которых отправлялись команды.

Таким образом, определение места совершения мошенничества в сфере компьютерной информации при установлении обстоятельств, подлежащих доказыванию, обладает определенной особенностью [4].

Перед началом осмотра места происшествия (компьютера, обстановки на месте преступления) следователь (дознаватель) обязательно должен принять меры, позволяющие предотвратить повреждения или уничтожения информации, следов преступления:

– осуществление постоянного электроснабжения ЭВМ в момент осмотра;

– удаление всех посторонних лиц с места происшествия и прекращение доступа к нему;

– ограничение и лишение доступа к техническим устройствам, источникам питания всех оставшихся лиц;

При проведении осмотра должны присутствовать специалист в области судебной компьютерно-технической экспертизы, специалист-криминалист для фиксации следов преступления на компьютерных средствах (следы рук).

Осмотр документов (источников и носителей криминалистически значимой компьютерной информации, документации, различных записей, даже на клочках бумаги) может иметь значение для успешного достижения цели.

Целесообразно осуществить допрос администратора системы (системного администратора) и выяснить: какие операционные системы установлены на каждом из компьютеров; какое используется про-

граммное обеспечение; какие применены системы защиты и шифрования; где хранятся общие файлы данных и резервные копии; каковы пароли супервизора и администраторов системы; какие зарегистрированы имена и пароли пользователей [8].

Еще одним важным следственным действием по данной категории преступлений является судебная компьютерно-техническая экспертиза, которая подразделяется на следующие виды:

а) судебная аппаратно-компьютерная экспертиза, заключающаяся в проведении исследования: технических (аппаратных) средств компьютерной системы: персональных компьютеров; периферийных устройств, сетевых аппаратных средств (серверы, рабочие станции, активное оборудование, сетевые кабели и т. д.); интегрированных систем (органайзеры, пейджеры, мобильные телефоны и т. п.); встроенных систем (иммобилайзеры, транспондеры, круиз-контроллеры и др.); любых комплектующих всех указанных компонентов (аппаратные блоки, платы расширения, микросхемы и т. д.);

б) судебная программно-компьютерная экспертиза, назначаемая для исследования программного обеспечения. Объекты включают: системное программное обеспечение; прикладное программное обеспечение (текстовые и графические редакторы, системы управления базами данных, электронные таблицы); авторское программное обеспечение потребительского назначения;

в) судебная информационно-компьютерная экспертиза, имеющая цель поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или порожденной программами для организации информационных процессов в компьютерной системе: базы данных и другие приложения, имеющие прикладной характер [9];

г) судебная компьютерно-сетевая экспертиза, основывающаяся прежде всего на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Задачи этой экспертизы включают практически все основные задачи рассмотренных выше видов экспертизы. Это объясняется тем, что ее объекты интегрированы из объектов рассмотренных выше видов экспертиз (аппаратные, программные и данные), но лишь с той разницей, что они все функционируют в определенной сетевой технологии.

По делам данной категории могут назначаться судебные экспертизы других классов и родов:

– судебно-трасологические – для анализа следов взлома, следов рук как на внешних, так и на внутренних поверхностях компьютеров и их комплектующих;

– судебно-технические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов, фальшивых денежных билетов и проч.;

– фоноскопические экспертизы – при использовании средств прослушивания переговоров и др.

В заключение отметим, что для обеспечения успешной борьбы с киберпреступлениями органам внутренних дел необходимо владеть современными цифровыми технологиями, активно использовать защитные программы для сохранности персональной информации, а также совершенствовать практику расследования киберпреступлений.

Среди мероприятий по борьбе с компьютерным мошенничеством необходимо выделить такие, как:

1) подготовка квалифицированных специалистов по противодействию киберпреступлениям;

2) создание «интеллектуальной системы», которая позволит автоматически вычислять в сети «Интернет» и помогать раскрывать киберпреступления в короткие сроки, что, безусловно, отразится на качестве предварительного расследования;

3) проведение профилактики среди населения о вреде выкладывания в сеть «Интернет» своих персональных данных;

4) улучшение систем защиты персональной информации.

Библиографический список

1. Электронный ресурс: https://мвд.рф/reports/item/12167987/ (дата обращения: 31.01.2018).

2. Электронный ресурс: https://мвд.рф/mvd/structure1/Centri /Glavnij_informacionno_analiticheskij_cen (дата обращения: 31.01.2018).

3. Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. – 2017. – № 280.

4. Третьяк М. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных главой 28 УК РФ // Уголовное право. – 2014. – № 4. – С. 51.

5. Третьяк М. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. – 2016. – № 2. – С. 23.

6. Электронный ресурс: https://rospravosudie.com/ (дата обращения: 31.01.2018).

7. Гончар В. В., Батюк В. И. Розыск лиц, скрывшихся от органов предварительного расследования // Вестник Московского университета МВД России. – 2006. – № 9. – С. 77.

8. Ефремова М. А. Мошенничество с использованием электронной информации // Информационное право. – 2013. – № 4. – С. 34.

9. Электронный ресурс: http://www.cdep.ru/index.php/ (дата обращения: 31.01.2018).

М. А. Потапенко[1], С. В. Ермаков[2]

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

За последнее десятилетие криптовалюты произвели настоящий фурор на мировую экономику. Еще недавно один «биткоин» стоил около 100 долларов, а сейчас его стоимость доходит до 15 тысяч долларов, и, естественно, большинство государств хочет урегулировать процесс оборота криптовалюты. Если оставить все как есть, то мы получим не отслеживаемые деньги.

Отметим страны, где разрешено использовать криптовалюты в качестве средства платежа:

1. Япония (легализовала).
2. Филиппины (признали платежным средством).
3. Малайзия (готовится легализовать).
4. Южная Корея (готовится легализовать).
5. Бельгия (обычные финансовые операции), не облагается налогом.
6. Финляндия (обычные финансовые операции), не облагается налогом.
7. Германия (законная валюта), облагается налогом.
8. Канада (обычные финансовые операции), не облагается налогом.
9. Великобритания (пытается установить контроль над биржами).
10. США (облагаются налогом).
11. Аляска (пытаются лицензировать криптовалютный бизнес).

---

[1] Курсант 421 учебного взвода Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Потапенко М. А., 2018.

[2] Заместитель начальника кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Ермаков С. В., 2018

12. Чехия (заняли нейтральную позицию).

13. Англия (Центральный банк попросил другие банки содействовать Блокчейн – проектам.).

14. Индия (готовится закон об использовании).

15. Франция (готовится закон об использовании).

С ростом популярности криптовалюты преступность взяла этот интернет-ресурс к себе на вооружение. По оценкам Интерпола и европейской полиции, популярность биткоинов и другой криптовалюты среди преступников стремительно растет и уже через несколько лет ее можно будет признать основным платежным инструментом в преступном мире.

Также вполне возможно, что с помощью криптовалюты возможно спонсирование терроризма, т. к. отсутствуют механизмы контроля данной финансовой деятельности [1, с. 132]. Ничто не мешает злоумышленникам перевести несколько сотен в биткоинов в различные страны, чтобы обналичить их.

Обратимся к зарубежному опыту выявления преступлений, где фигурирует криптовалюта.

1. В декабре 2013 г. Эндрю Густафсон создал в глубоком Интернете сайт Community X, посвященный производству в Уганде поддельных банкнот Федеральной Резервной Системы. Он активно продвигал банкноты и продавал их за биткойны через онлайн-форумы, затем их сбывали в кофейнях и магазинах США и Уганды. Кроме того, рабочая группа обнаружила непроверенную информацию о лицах, обманутых неофициальными онлайн-биржами Уганды при обмене биткойнов.

2. В конце июля 2017 г. в Греции по запросу Минюста США был задержан россиянин Александр Винник – ключевая персона в организации одной из старейших бирж криптовалют BTC-e. В пресс-релизе на сайте Минюста США говорится, что его подозревают в предоставлении нелегальных финансовых услуг и отмывании денег. По данным полиции, якобы возглавляемая россиянином преступная организация с 2011 г. легализовала до $4 млрд. Своими действиями, считают правоохранительные органы США, Винник, способствовал наркоторговле, краже личных данных, а также помогал легализовать незаконные доходы преступных группировок по всему миру. Обвинение называет Винника владельцем и оператором многочисленных учетных записей биржи BTC-e, в том числе учетных записей с правами администратора, а также как бенефициара управляющей биржей оффшорной компании Canton Business Corporation.

В России есть две основные проблемы, связанные с криптовалютой: отсутствие правового регулирования криптовалют и отсутствие методики расследования преступлений, связанных с криптовалютой.

Начнем с первой проблемы. Какие есть правовые основания для использования криптовалюты в России? Само понятие криптовалюты не поименовано в числе объектов гражданских прав, предусмотренных ст. 128 Гражданского кодекса Российской Федерации, имеющих необходимую гражданскую «оборотоспособность». Объектами гражданских правоотношения являются вещи, включая наличные деньги и ценные документарные бумаги, иное имущество, в том числе безналичные денежные средства, ценные бездокументарные бумаги, имущественные права, результаты работ и оказание услуг, охраняемые результаты интеллектуальный деятельности и приравненные к ним средства интеллектуальной собственности, нематериальные блага.

Наиболее очевидным выходом из сложившейся ситуации выглядит попытка приравнять криптовалюту к деньгам ввиду содержательного сходства и применить соответствующий правовой институт по аналогии. Однако при более тщательном анализе подобная аналогия оказывается несостоятельной по трем причинам.

Во-первых, предметом преступления против собственности являются любые физические предметы, любое имущество, не исключенные из общегражданского оборота и имеющие потребительскую стоимость.

Во-вторых, все деньги отнесены законодателем к имуществу, при этом наличные деньги – к вещам, а безналичные денежные средства – к иному имуществу.

В-третьих, в соответствии со ст. 140 ГК РФрубль является законным платежным средством, обязательным к приему по нарицательной стоимости на всей территории Российской Федерации. Порядок и условия использования иностранной валюты на территории Российской Федерации определяются законом или в установленном им порядке.

Хоть и отсутствует правовое регулирование у данной «валюты», однако первое преступление в России уже было совершенно с помощью нее. Так, 1 сентября 2017 года стало известно о возбуждении в Костроме первого в России уголовного дела в отношении троих участников группы, осуществляющих майнинг биткойнов и их продажу в Интернете [4].

Указанным лицам инкриминируется совершение преступления, предусмотренного ч. 2 ст. 172 Уголовного кодекса Российской Феде-

рации, т. е. незаконная банковская деятельность, совершенная организованной группой и сопряженная с извлечением дохода в особо крупном размере. Данная норма предполагает наказание вплоть до лишения свободы на срок до семи лет.

Теперь перейдем непосредственно ко второй проблеме. Какие могут быть в будущем преступления, связанные с криптовалютой? Так, например, гражданин может заниматься получением доходов с «криптовалютного» сайта, но злоумышленники узнали пароль от аккаунта гражданина и похитили средства с его личного кабинета на сайте «криптовалютной» биржи. Затем данный актив перечислили на другой счет. В данном случае предстоит расследовать преступление по ст. 158 УК РФ. Квалификация по соответствующей части данной статьи будет происходить в зависимости от размера похищенных денежных средств с «криптовалютного» счета гражданина.

Следователь (дознаватель) должен будет произвести в соответствии с ч. 3.1 ст. 183 УПК РФ выемку, осуществив изъятие электронных носителей информации. Необходимо установить, был ли осуществлен незаконный доступ к данному компьютеру. Запросить отчет с сервера сайта о последних входах в аккаунт гражданина и затем (если удалось получить отчет) выяснить местоположение преступника по IP-адресу. В случае, если это сделали за границей, то необходимо сделать запрос в Интерпол.

Рассмотрим иную ситуацию. Например, должностному лицу предложили взятку в виде биткоинов за оказание услуги в рамках его полномочий. Должностное лицо соглашается и просит перевести на его аккаунт деньги. Полагаем, что дознаватель (следователь) должен наложить арест на имущество (криптовалюту) по судебному решению, т. к. это можно рассматривать как имущество, находящееся на счете. Дознавателю (следователю) необходимо выяснить, с какого счета была переведена данная сумма. Для этого потребуется назначение судебной компьютерно-технической экспертизы или помощь специалиста [2, с. 28].

К сожалению, надежных методик и рекомендаций по расследованию преступлений, связанных с криптовалютой, еще не разработано.

Полагаем, что Россия также должна пользоваться криптовалютой в экономической деятельности, но для этого нужно сделать несколько серьезных решений:

Включить в действующее законодательство понятие «виртуальные деньги» или «криптовалюта». Данное понятие можно заимствовать из

определения виртуальной валюты, данное в законе штата Нью-Йорк о регулировании виртуальных валют.

Ввести налогообложение майнинговых операций.

Разработать методики наложения ареста на криптовалюту. Создать криптовалютные счета органов предварительного расследования для хранения изъятых в ходе процессуальных действий криптовалют.

Обеспечить подготовку специалистов, способных к расследованию киберпреступлений [3, с. 18].

Библиографический список

1. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130-135.

2. Ермаков С. В. Проверка сообщений о преступлениях экономической направленности: пути совершенствования законодательства // Научный портал МВД России. – 2017. – № 2. – С. 26.

3. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 18.

4. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – № 2 (20). – С. 30–38.

***А. А. Орлова*[1]**

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ ИЗ БАНКОВСКИХ АВТОМАТИЧЕСКИХ ТЕРМИНАЛОВ САМООБСЛУЖИВАНИЯ

С развитием банковской системы и электронных технологий, в период повсеместного распространения безналичных расчетов и электронных платежных систем банкоматы как один из основных элементов автоматизации процессов банковских операций все чаще используются для совершения преступлений.

Следует подчеркнуть, что ввиду многообразия проявлений признаков объективной и субъективной стороны совершаемых в указанной сфере преступлений правоприменительная практика сталкивается

[1] Главный научный сотрудник НИЦ № 5 ФГКУ «ВНИИ МВД России» доктор юридических наук, доцент. © Орлова А. А., 2018.

в целях рядом сложностей, связанных не только с квалификацией противоправных действий, но и со своевременным и правильным выявлением способа получения неправомерного доступа к сведениям, составляющим налоговую [1], коммерческую [2] или банковскую [3] тайну юридических и физических лиц с целью последующих хищений их денежных средств, с надлежащим процессуальным оформлением полученной информации, с доказыванием обстоятельств, предусмотренных в ст. 73 УПК РФ.

Остановимся лишь на некоторых из обозначенных аспектов проблем.

Одним из способов получения персональных данных и хищений денежных средств граждан является установка на банкоматы так называемого внештатного оборудования. При этом наиболее распространенным способом получения персональных данных клиентов небезосновательно считается скимминг.

Под скиммингом следует понимать копирование данных путем установки перед картридером[1] специального устройства – «скиммера». Данное устройство по своему внешнему виду имитирует стандартное оборудование банкомата и визуально не распознается лицом, желающим получить принадлежащие ему денежные средства из банкомата по персонифицированной банковской карте.

Как правило, сбор сведений о персональных данных владельцев банковских карт, а также сведения об их ПИН-кодах, осуществляется для последующего хищения денежных средств со счетов граждан – владельцев скомпрометированных карт.

Следовательно, при проверке заявлений и сообщений о преступлениях, связанных с хищением из банкоматов или с их использованием путем скимминга органам предварительного расследования необходимо учитывать целый ряд обстоятельств, позволяющих ориентироваться в вопросах установки и использования указанного вида внештатного оборудования, а также его обнаружения и надлежащей процессуальной фиксации полученных результатов.

Как правило, факты, свидетельствующие об установке скиммера на банкомате, выявляются сотрудниками банков при их осмотре, а также в результате обращений пострадавших граждан о хищении денежных средств.

---

[1] Под картридером понимается небольшое по размеру устройство, предназначенное для быстрого считывания карт памяти, compact flash карточек и других типов памяти.

Совокупность первоначальных процессуальных действий и организационных мероприятий при наличии надлежащего, предусмотренного в ст. 140 УПК РФ повода для возбуждения уголовного дела, включает в себя: выезд следственно-оперативной группы на место совершения преступления; получение объяснений; истребование и получение сведений о движении денежных средств по соответствующим банковским счетам; проведение осмотра места происшествия.

Принимая во внимание, что выезд на место происшествия предполагает выполнение действий, связанных с высокотехнологичным оборудованием, а обнаружение и изъятие значимых для расследования преступления предметов требуют специальной подготовки и должной квалификации, результаты производимых мероприятий определяются не только квалификацией следователя, но и уровнем и профилем профессиональной подготовки соответствующего специалиста, что необходимо учитывать при формировании оперативно-следственной группы.

Как показывает практика, проведение осмотра места происшествия при проверке сообщений об установке и использовании скиммера вызывает особую сложность. Это обусловлено необходимостью правильно определить границы осмотра, круг участников следственного действия; многообразием производимых действий, направленных на обнаружение, изъятие, надлежащую упаковку предметов, имеющих значение для дела, и оставленных на месте совершения преступления следов, фиксацию и протоколирование производимых действий, соблюдение прав участвующих лиц.

УПК РФ (ст. ст. 176, 177, 180) регламентирует общие и обязательные требования, предъявляемые к процедуре проведения указанного следственного действия, которые необходимо учитывать при его осуществлении в целях придания в дальнейшем полученным результатам статуса доказательств, в то время как необходимая и достаточная в каждом случае совокупность действий, равно как и их последовательность, определяются следователем.

Поэтому ввиду сложности осмотра места происшествия применительно к выявлению и идентификации в банкомате внештатного оборудования, необходимо исходить из целого ряда практических рекомендаций, позволяющих правильно оценить обстановку.

Так, например, в целях обнаружения таких скимминговых устройств, как видеокамеры, накладки на клавиатуру, приспособления, считывающие магнитные полосы, а также следов их установки (клей,

скотч и т. д.), иных предметов, имеющих значение для дела, следует произвести осмотр не только банкомата и непосредственно находящихся поблизости объектов, но и прилегающей территории.

Вблизи банкомата может находиться использованный преступниками автотранспорт с имеющими отношение к внештатному оборудованию техническими устройствами (видеокамеры, накопители информации, ноутбуки, планшеты, флэш-карты, навигаторы, мобильные телефоны, сим-карты и т. д.).

В ходе осмотра места происшествия изымают записи камер видеонаблюдения.

Осмотр места происшествия производится в присутствии представителя банка, с участием специалиста. При отсутствии понятых закон предусматривает необходимость применения технических средств фиксации его хода и результатов (ч.1^1 ст. 170 УПК РФ).

Однако в случаях осмотра места происшествия в рамках проверки сообщений об установке и использовании скиммера, фото-, видеофиксация производимых действий представляется обязательной независимо от присутствия понятых, о чем участники следственного действия предупреждаются до начала его проведения, а сведения о применяемых технических средствах, об условиях и порядке их использования, об объектах, к которым они были применены, должны быть указаны в протоколе следственного действия (ст. 166 УПК РФ).

Банкомат, оборудование, имеющие отношение к делу другие предметы, автотранспорт, проверяются на наличие следов рук, потожировых и иных следов, оставленных человеком, которые в случае их обнаружения должны быть изъяты, упакованы с указанием индивидуальных признаков, опечатаны и заверены подписью компетентного должностного лица на месте осмотра происшествия (ч. 3 ст. 177 УПК РФ).

Все подлежащие изъятию обнаруженные предметы предъявляются участникам следственного действия.

Значимыми для решения вопроса о возбуждении уголовного дела и последующего расследования являются сведения из банка, которому банкомат принадлежит. Данные сведения подтверждаются выписками из расчетных счетов пострадавших лиц и соответственно содержат информацию о хищениях денежных средств клиентов.

Из заявлений и объяснений граждан о хищении у них денежных средств могут быть установлены обстоятельства, имеющие решающее значение для решения вопроса о возбуждении уголовного дела, в том числе подтверждающие факт установки скиммера, незаконного полу-

чения сведений, составляющих банковскую тайну лица, и хищение его денежных средств, место и время совершения указанных действий.

В тех ситуациях, когда уголовное дело возбуждается в результате задержания лица при установке или снятии внештатного оборудования, следует учитывать значение выяснения обстоятельств его приобретения, использования, цели установления, выявления круга соучастников и видов соучастия, возможных мест нахождения причастных к преступлению лиц, адресов, телефонов, мест изготовления дубликатов карт, мест и времени передачи незаконно полученной информации, носителей ее содержащих для изготовления дубликатов карт.

После возбуждения уголовного дела в числе следственных действий приоритетное значение приобретает проведение обыска с целью обнаружения, например, дубликатов кредитных карт, оборудования, предназначенного для несанкционированного считывания информации с банковских карт или приспособленного для изготовления его элементов, компьютерной техники и т. д.

По общему правилу обыск в жилище проводится по судебному решению. Для этого следователь с согласия руководителя следственного органа выносит постановление о возбуждении перед судом ходатайства о производстве обыска.

Принимая во внимание, что при расследовании преступлений с использованием внештатного оборудования под подозрение в причастности к их совершению попадает достаточно широкий круг лиц, в каждом случае возбуждения соответствующего ходатайства надлежит обращать самое серьезное внимание на содержание описательно-мотивировочной части постановления, из содержания которой исчерпывающим образом должны усматриваться законность, обоснованность и необходимость проведения обыска у конкретного лица. Это позволит судье принять надлежащее решение без затребования дополнительных сведений и соответственно в кратчайшие сроки.

Однако в исключительных случаях проведение обыска допускается в порядке, предусмотренном ч. 5 ст. 165 УПК РФ – по постановлению следователя с последующим уведомлением судьи и прокурора о его производстве. Здесь необходимо учитывать, что к уведомлению прилагаются копии постановления о производстве следственного действия и протокол следственного действия, что накладывает на должностных лиц обязанности как по надлежащему обоснованию законности и обоснованности его производства без судебного решения, так и по надлежащему процессуальному оформлению его хода и результатов.

В противном случае все полученные в ходе такого следственного действия доказательства признаются недопустимыми в соответствии со ст. 75 УПК РФ.

Важным направлением деятельности следователя при расследовании преступлений, совершаемых с использованием скимминговых устройств, является назначение экспертиз, среди которых важное место занимают компьютерная, химическая, бухгалтерская, портретная, дактилоскопическая.

В соответствии с ч. 1 ст. 144 УПК РФ назначить судебную экспертизу и получать заключение эксперта можно до возбуждения уголовного дела, т. е., в ходе проверки сообщения о преступлении.

Однако следует учитывать, что перечень прав, указанных в ч. 1 ст. 198 УПК РФ, которыми наделены подозреваемый, потерпевший, свидетель при назначении и производстве судебной экспертизы, имеет под собой объективные основания на этапе предварительного расследования, т. е. применительно к конкретно определенному кругу лиц, наделенных соответствующим процессуальным статусом.

В то же время до возбуждения уголовного дела они таким статусом не обладают. В связи с этим а также исходя из целесообразности разглашения сведений, связанных с назначением соответствующих экспертиз лицам, не обладающим конкретно определенным процессуальным статусом, на данном этапе уголовного судопроизводства реализация совокупности прав, указанных в ч. 1 ст. 198 УПК РФ, представляется избыточной.

При этом следует подчеркнуть необходимость соблюдения прав участников уголовного судопроизводства для получения допустимых доказательств в результате проведения следственных действий, что, безусловно, надлежит учитывать при решении вопроса о целесообразности назначения и производства судебной экспертизы на соответствующем этапе уголовного судопроизводства.

Помимо изложенного надлежит обратить внимание на вопросы квалификации преступлений, совершенных с использованием автоматических терминалов самообслуживания, наиболее распространенными из которых, как показывает практика, на текущий момент являются хищения денежных средств по скомпрометированным банковским картам.

Вместе с тем, необходимо учитывать, что хищению денежных средств из банкоматов путем установки и использования внештатного оборудования предшествует совокупность действий, направленных на

незаконное получение (разглашение) сведений, составляющих коммерческую, налоговую или банковскую тайну соответствующего лица, указанных в ст. 183 УК РФ, предусматривающей уголовную ответственность за их собирание незаконным способом.

Поэтому действия лиц, получающих неправомерный доступ к охраняемой законом тайне – персональным данным владельцев банковских карт при помощи внештатного оборудования, следует квалифицировать по соответствующей части данной статьи.

Вместе с тем квалификация деяния может определяться моментом выявления преступления. Так, например, в случае задержания лица при установке или снятии скимминговых устройств уголовное дело возбуждается по ч. 3 ст. 30 (покушение на преступление) и соответствующей части ст. 183 УК РФ, а впоследствии при установлении фактов, свидетельствующих о совершении преступления, привлечение в качестве обвиняемого предполагает квалификацию фактически осуществленных действий по ст. 183 УК РФ в той части, которой они соответствуют. В тех случаях, когда после получения несанкционированного доступа к персональным данным владельцев персональных банковских карт с их счетов были похищены денежные средства, содеянное квалифицируют по совокупности ст. ст. 183 и 158 УК РФ.

При этом необходимо учитывать, что хищение денежных средств из банкомата путем использования заранее похищенной или поддельной платежной карты без участия уполномоченного работника кредитной организации следует квалифицировать, как тайное хищение чужого имущества (кража) по соответствующей части ст. 158 УК РФ [4], т. е. разграничивать с мошенничеством.

Следует отметить, что в последнее время количество преступлений, связанных с хищениями из банковских автоматических терминалов самообслуживания с использованием внештатного оборудования, несколько уменьшилось. Во-первых, банковское сообщество отреагировало на сложившуюся криминогенную ситуацию и установило оборудование с устройствами, которые выдают денежные средства только с карт, имеющих встроенные чипы, что значительно осложнило возможности «реализации» данных, полученных с использованием скимминговых устройств. Во-вторых, нельзя не признать успешную деятельность правоохранительных органов по выявлению и расследованию преступлений, задержанию и привлечению к ответственности лиц, занимающихся созданием, установкой и использованием внештатного оборудования в преступных целях.

Вместе с тем, количество хищений по-прежнему остается значительным в ходе неправомерного использования реквизитов персонифицированных банковских карт, их ПИН-кодов, номеров и т. д., которые становятся известны преступникам, например, при оплате товара в Интернете, переводе денег с одного счета на другой.

Кроме того, в средствах массовой информации предупреждают о возможности использования в период проведения чемпионата мира по футболу банкоматов, приобретенных для скимминга на вторичном рынке, которые могут быть визуально замаскированы под банкоматы известных банков. Если клиент попытается снять деньги в таком банкомате, он получит сведения об ошибке, в то время, как данные его банковской карты станут известны преступникам. При этом, поскольку данный банкомат фактически не будет принадлежать ни одной официальной банковской структуре, вопрос о возврате денег станет проблематичным [5].

Изложенное свидетельствует о необходимости постоянного расширения объема знаний, необходимых для совершенствования правоприменительной деятельности, что предполагает взаимообмен опытом с сотрудниками безопасности финансово-кредитных учреждений [6], в том числе и в ходе научных конференций, использование уже разработанных и разработка новых, соответствующих реалиям криминогенной обстановки в указанной сфере методических рекомендаций.

Библиографический список

1. Налоговый кодекс Российской Федерации, часть первая от 31.07.1998 г. № 146-ФЗ (ред. от 29.12.2017 г.), ст. 102 // СПС «КонсультантПлюс».

2. Федеральный закон «О коммерческой тайне» от 29 июля 2004. № 98-ФЗ, ст. 3 // СПС «КонсультантПлюс».

3. Федеральный закон «О банках и банковской деятельности» от 03.02.1996 г. № 17-ФЗ (в ред. от 31.12.2017 г. № 482-ФЗ), ст. 26 // СПС «КонсультантПлюс».

4. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // www.garant.ru.

5. Коммерсантъ. – 2018. – 29 января.

6. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 134.

В. И. Ткачева[1], Т. В. Радченко[2]

ОСОБЕННОСТИ ДОПРОСА СВИДЕТЕЛЕЙ ПО ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ IT-ТЕХНОЛОГИЙ

Мировое сообщество рассматривает киберпреступность как глобальную международную проблему, о чем свидетельствуют принятые в последние годы международные договоренности, которые предусматривают совместные усилия по борьбе с этим высокотехнологичным злом. По мнению экспертов ООН, под киберпреступностью следует понимать любое противозаконное действие, совершаемое в виртуальном пространстве [1]. Опасность киберпреступности как для мирового сообщества в целом, так и для России является очевидной. Так, по данным Главного управления специальных технических мероприятий МВД России, киберпреступность в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере [2].

Преступления, совершаемые в этой сфере, обладают рядом специфических признаков:

– как правило, такие деяния имеют высокий уровень латентности: применение анонимайзеров либо выход в сеть через «подставные компьютеры» (например, в интернет-кафе) – все это делает практически невозможным установление личности преступника;

– для подобных преступных деяний свойственна так называемая трансграничность. Иными словами, преступник и его «жертва» могут находиться на любом удалении друг от друга, для выполнения каких-либо действий во взаимодействии между ними нет необходимости;

– преступления совершаются, как правило, в автоматизированном режиме. Хакерами разработаны и «вполне успешно» (с точки зрения криминальной направленности) применяются программы, которые автономно позволяют осуществлять незаконный перевод денежных средств со счетов ничего не подозревающих компаний и граждан;

– рассматриваемым деяниям свойственна нетипичность или нестандартность действий преступников [3];

---

[1] Курсант 4 В курса Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Ткачева В. И., 2018.

[2] Преподаватель кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Радченко Т. В., 2018.

В отличие от обычных преступлений при совершении преступлений с использованием возможностей IT-технологий зачастую довольно трудно установить признаки объективной стороны деяния, не говоря уже про выявление, обнаружение и задержание преступников.

Исследователи выделяют отдельные трудности расследования преступлений, совершаемых с использованием возможностей IT-технологий:

– зачастую правоохранительным органам не сразу удается выявить сам факт правонарушения. Преступники с особой легкостью могут получить информацию, которая скрыта, и об этом никто не узнает;

– степень причиненного вреда может быть очень значительна: злоумышленник может взломать целую базу данных какого-нибудь банка и снять денежные средства со счетов клиентов;

– преступник, который совершил деяние на территории России, может быть из любой точки мира;

– интеллектуальная составляющая данного вида преступной деятельности довольно высока. Как правило, преступники наделены незаурядным интеллектом, умеют хорошо скрывать следы, что создает сложности в борьбе против них.

Тактика производства допроса свидетелей при расследовании киберпреступлений напрямую зависит от многих факторов как позитивных, так и негативных. Опросы следователей расследующих данную категорию дел показывают, что они часто сталкиваются со сложностями при допросе. Около 71 % опрошенных указали, что чаще всего трудности возникают с терминологией, а также с выбором тактики воздействия и установлением контакта с допрашиваемым [4].

При подготовке к допросу и в ходе его проведения следователю необходимо обратить внимание, во-первых, на возможность привлечения специалистов, которые обладают специальными знаниями в сфере телекоммуникационных систем, компьютерных технологий и компьютерной техники, так как зачастую следователи не обладают такими знаниями или обладают ими в недостаточном объеме. Отсутствие специальных знаний у следователя обусловливает «интеллектуальное» противодействие расследованию со стороны преступника [5]. Во-вторых, на постоянную изменчивость сетевого пространства, которое в свою очередь определяется краткосрочностью существования и высокой изменчивостью отдельных видов доказательств, находящихся в электронной форме. При производстве допроса следователю целесообразно применять знания юридической психологии, поскольку имен-

но применение психологических приемов позволяет расположить к себе допрашиваемого свидетеля и получить от него максимум информации. Также, готовясь к допросу свидетеля по киберпреступлениям, следователю нужно обратить особое внимание на информационное обеспечение допроса и планирование самой процедуры допроса. Одной из наиболее важных составляющих является информационное обеспечение: чем оно технологичнее, тем выше степень контроля ситуации на допросе. Это в свою очередь позволит избежать ошибок в квалификации преступного деяния.

Положительно на выбор тактических приемов производства допроса влияет достаточная осведомленность следователя о типах и видах компьютерно-технических средств, выступивших в качестве орудия совершения преступления.

Именно это обстоятельство по общему правилу обусловливает необходимость присутствия при производстве следственных действий (допроса) специалиста в сфере компьютерных технологий, который уже на стадии подготовки к допросу может разъяснить следователю неясные технические термины, особенности устройства и принцип работы изъятых средств, возможные способы совершения преступлений посредством их применения.

При производстве допроса при расследовании киберпреступлений основной целью является выявление (выяснение) информации, связанной с виртуальными следами, а также иной информации, имеющей отношение к расследуемому виду киберпреступления.

Как отмечалось выше, допрос свидетелей имеет тактические особенности, которые зависят не только от механизма совершения киберпреступлений, но и от криминалистического типа свидетелей.

Тактика производства допроса по уголовным делам этой категории напрямую зависит от специфики механизма совершения преступления и иных как позитивных, так и негативных факторов. К числу первых следует отнести наличие определенного объема информации о преступном событии, полученного из различных источников (в ходе предварительной проверки материалов о расследуемом событии, результаты оперативно-разыскных мероприятий), а также о лице, с которым предстоит производство следственного действия (полученной ранее в ходе его объяснений, из протоколов процессуальных действий). В число негативных факторов можно включить значительный промежуток времени, прошедший с момента совершения преступления до момента производства допроса [6].

Представляется обоснованной точка зрения В. М. Быкова, который считает, что тактика допроса должна строиться с учетом соответствующего криминалистического типа допрашиваемых. Им были выделены следующие типы: активные и неактивные, добросовестные потерпевшие, неустойчивые, недобросовестные потерпевшие [7].

Данную типизацию можно применить и к свидетелям. Так, например, допрашивая свидетелей, необходимо выяснить следующую информацию: какие компьютерно-технические средства использовались потерпевшим или подозреваемым; какими знаниями о компьютерно-технических средствах, их характеристиках обладают допрашиваемые; какими навыками работы на компьютере или технически сложном устройстве владеют. В процессе их допроса необходимо установить: местонахождение юридического лица, организационно-правовую форму и характер деятельности; режим деятельности юридического лица; содержание и объем информации, хранящейся в компьютере; кто из сотрудников и каким образом вступал в контакт с предполагаемыми преступниками, и другое. Данный перечень зависит от конкретной типичной исходной следственной ситуации и не является исчерпывающим.

Таким образом, тактически значимая информация о личности киберпреступников при производстве допроса свидетелей должна быть направлена на установление и получение сведений об уровне технической подготовленности и компьютерных навыках подозреваемых; о возможных мотивах совершения киберпреступления; о дифференциации в зависимости от локализации преступной деятельности; об информации, размещенной в социальных сетях; о психологическом состоянии или информационных болезнях (зависимостях, фобиях) подозреваемых.

Тактика производства допроса по уголовным делам этой категории напрямую зависит от специфики механизма совершения киберпреступлений [8].

Таким образом, специфика расследования преступлений, совершенных с использованием возможностей IT-технологий требует разработки новых тактических подходов и приемов к осуществлению такого следственного действия как допрос, что без сомнения позволит повысить эффективность расследования [9].

Библиографический список

1. Доклад Управления ООН по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности». 2013. // http://pdf.knigi-x.ru/21yuridicheskie/136262-1-unp-oon-upravlenie-organizacii-obedinennih-naciy-narkotikam-prestupnosti-vsestoronnee-issle.php.

2. http://www.crime-research.ru/library/Mirosh1.html.

3. Свистун С. Н. Особенности проведения допроса (очной ставки) при расследовании киберпреступлений // Экономика и социум. – 2017. – № 8 (39). – С. 26. http://www.iupr.ru.

4. Шевченко Е. С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. – 2016. – № 10. – С. 160–169.

5. Яковлев А. Н., Олиндер Н. В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. – М., 2012. – С. 43.

6. Смирнова И. Г., Коломинов В. В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Известия Иркутской государственной экономической академии. Электронный научный журнал. – 2015. – Т. 6. – № 3. http://eizvestia.isea.ru.

7. Быков В. М. Допрос потерпевшего // Законность. – 2014. – № 6. – С. 27–32.

8. Маслакова Е. А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. – 2014.– № 1. – С. 36.

9. Орлова А. А., Батюк В. И., Мешков М. В. и др. Предварительное следствие в органах внутренних дел : учебное пособие / под ред. М. В. Мешкова. – М. : Щит-М, 2007. – С. 285.

М. В. Разинькова[1], *В. Ю. Иванов*[2]

ПРОБЛЕМЫ ИЗЪЯТИЯ МОБИЛЬНЫХ УСТРОЙСТВ ПРИ ПРОВЕДЕНИИ СЛЕДСТВЕННОГО ДЕЙСТВИЯ «ОБЫСК»

Расширение сферы применения современных информационных технологий, появление новых видов преступлений приводят к тому, что при расследовании уголовных дел в ходе проведения осмотров, выемок, обысков все чаще возникает необходимость изъятия электронных носителей информации, содержащих данные, которые впоследствии могут быть использованы в доказывании.

Так, основой успешного изъятия электронных носителей информации, а также сохранение хранящейся на ней информации является участие специалиста при производстве данного следственного действия. Данному важному факту часто не придают значение следователи либо другое лицо, которое ведет дело. Не принимая это во внимание, создается риск пропажи, уничтожения и модификации значимой информации для разрешения дела, раскрытия и предотвращения преступления.

Наряду с описанным выше, существует еще одна очень важная проблема в затронутой области. В настоящее время в структуре МВД Российской Федерации нет утвержденных методических рекомендаций для специалиста, который участвует в следственном действии «Обыск», связанном с изъятием электронных носителей информации. Отсутствие данных методик существенно затрудняет построение специалистом своей тактики действий при участии в следственном действии «Обыск».

В ст. 182 УПК РФ: обыск – это следственное действие, заключающееся в обследовании помещений, участков местности и граждан в целях отыскания и изъятия предметов, документов, ценностей и (или) трупа, могущих иметь значение для уголовного дела, свидетельств их принадлежности конкретному лицу, а равно для отыскания разыскиваемой личности – задержания правонарушителя либо освобождения потерпевшего.

---

[1] Слушатель 518 учебного взвода 5 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Разинькова М. В., 2018.

[2] Доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя кандидат технических наук. © Иванов В. Ю., 2018.

Сферы использования электронных носителей информации весьма разнообразны, но хотелось бы выделить именно криминальную. На сегодняшний день при подготовке, совершении, сокрытии виновно опасного общественного деяния (далее преступление), преступник оставляет следы своей деятельности на электронных носителях информации.

Мобильные телефоны предназначены для работы в сетях сотовой связи, используя радиоканал для связи с абонентским устройством. Имеют большое разнообразие моделей, позволяющих в меру своей функциональной комплектации использовать как возможности информационно-коммутационных сетей, в том числе Интернет, так и возможности установленного программного обеспечения.

Обладает индикационными признаками – маркировочными обозначениями: самого мобильного телефона (название, модель, объем памяти, международный идентификатор мобильного оборудования IMEI); SIM-карты (название мобильного оператора, идентификационный номер); встраиваемой карты памяти (SD, SDHC, MMC, microSD, M2 MemoryStick) (название, модель, объем памяти, идентификационный номер).

Мобильный телефон как сложное высокотехнологичное электронное устройство может хранить в себе значимую информацию в следующих объектах:

– *Телефонная книга* – список мобильных номеров с инициалами их владельца, может также включать фотографии, пользовательские метки, даты дней рождения, профиль в социальных сетях.

– *Сообщения* – отправленные и полученные SMS, MMS, электронные письма, переданные по Bluetooth сообщения и их вложения, голосовые сообщения.

– *Звонки* – входящие и исходящие вызовы с других мобильных устройств.

– *Веб-соединения* – сессии GPRS и WiFi владельца устройства, точки доступа.

– *Аудиофайлы* – записи, музыка, мелодии и другие звуковые файлы.

– *Видеофайлы* – видеозаписи, сделанные как самим пользователем, так и загруженные им.

– *Изображения – фотографии*, сделанные самим пользователем, так и загруженные им, фотографии из социальных сетей, а также рисунки.

– *Заметки – записи пользователя*.

– *Календарь* – может включать в себя даты встреч, годовщин и прочих событий.

– История Веб-браузеров – ссылки, куки, загруженные файлы.

Данные установленных приложений: социальных сетей (VK, Instagram, Tinder, Twitter, Одноклассники и др.) – отправленные и полученные сообщения, голосовые сообщения, изображения, «прилепленные» файлы, геолокационные данные, видеозаписи; мессенджеры (Viber, Telegram, WhatsAppMessengerидр.) – списки контактов, отправленные и полученные сообщения, вызовы, прикрепленные файлы: фотографии, изображения, видеозаписи, документы; прочее программное обеспечение – игры, приложения управления финансами и т. д.

В данную группу можно также включить планшетные компьютеры, в том случае, когда они оснащены модулями 3G, 4G, LTE и GSM, а также используется SIM-карта с услугами сотовой связи.

Информация, хранимая в памяти данных устройств, будет схожа с мобильными телефонами, однако если планшетный компьютер будет оснащен только модулем для высокоскоростной передачи данных в сети «Интернет», услуги сотовой сети будут не доступны, а значит, и информация о деятельности пользователя в сотовой сети будет отсутствовать [1].

Осмотр мобильного телефона на предмет нахождения в его памяти информации, важной для следствия, целесообразно провести на месте, в тех случаях, когда специалист обладает портативной цифровой платформой, которая позволит ему получить доступ и извлечь из мобильного телефона всю хранимую информацию.

Осмотр мобильных телефонов на месте также необходим на тот случай, когда он защищен парольной защитой. В таком случае необходимо сообщить о данном факте лицу, которое проводит данное следственное действие. При изъятии мобильных устройств необходимо:

– извлечь из корпуса мобильного устройства SIM-карту (-ты);

– необходимо отключить парольную защиту, если телефон находится во включенном состоянии;

– поставить мобильное устройство в авиа режим, отключить передачу данных;

– произвести выключение мобильного устройства;

– если телефон выключен, произвести его включение, проверить наличие парольной защиты, если имеется, сообщить лицу, проводящему обыск;

– сообщить лицу, проводящему обыск, что для дальнейшего успешного исследования мобильного устройства необходимо узнать пароль от резервной копии (если такая имеется);

– упаковать и опечатать мобильное устройство.

Библиографический список

1. Васильева Е. А., Пузарин А. В., Захаров Д. Н. Исследование возможности применения биллинговых записей // Технологии информационной безопасности в деятельности органов внутренних дел. Сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 52–55.

П. Е. Власов[1]

ОСОБЕННОСТИ ПРОИЗВОДСТВА ДОПРОСОВ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ МОБИЛЬНЫХ МОШЕННИЧЕСТВ

Специфика совершения рассматриваемых преступлений позволяет преступникам удаленно завладеть денежными средствами со счетов банковских карт, используя мобильные средства связи, в условиях, исключающих личный контакт с потерпевшим.

Согласно статистическим данным за 2016-2017 гг., из общего массива преступлений, совершенных с использованием компьютерных и информационно-коммуникационных технологий, подследственных органам дознания, только по 11 % преступлений уголовные дела направлены в суд, а более чем по 60 % из общего числа преступлений, по которым были возбуждены уголовные дела, судебной перспективы не имеют и приостановлены производством по п. 1 ч. 1 ст. 208 УПК РФ. Уровень преступности данного вида имеет достаточно высокую тенденцию роста.

Увеличение количества рассматриваемых преступлений, а также причины несвоевременного и неполного их раскрытия носят как объективный, так и субъективный характер, и в основном связаны со сложностью квалификации действий виновных лиц, появлением новых, организационно многоуровневых способов совершения мошен-

[1] Начальник второго отдела по исследованию уголовно-процессуальных проблем Научно-исследовательского центра № 5 (по исследованию проблем расследования преступлений органами предварительного следствия и дознания) ФГКУ «ВНИИ МВД России» кандидат юридических наук, доцент. © Власов П. Е., 2018.

нических действий, совершенствованием виновными лицами системы противодействия их раскрытию. Кроме того, при расследовании возникают трудности в установлении местонахождения виновных лиц, места совершения преступления, в отыскании, закреплении, исследовании и использовании в доказывании следов преступления, неполноты проведенного расследования и низкого взаимодействия с оперативными подразделениями.

Лица, совершающие хищения денежных средств с использованием электронных платежных инструментов, используя полученную информацию и современные технологии, вынуждают потерпевших раскрывать информацию о своей личности, платежных картах, совершать переводы денежных средств на их счета как минимум двумя способами: первый – с помощью SMS-сервиса оператора мобильной связи; второй – с помощью использования специального мобильного приложения «Мобильный банкинг»[1] устанавливаемого на мобильное средство связи, через соответствующий официальный магазин мобильных приложений – «Appstore» и «GooglePlay»[2].

Основными следственными действиями [1], которые необходимо провести в каждом конкретном случае расследования уголовного дела о рассматриваемых преступлениях на первоначальном этапе, в условиях отсутствия достоверной информации о лице, совершившем данное преступление, будут допросы потерпевшего и свидетелей.

Допрос потерпевшего. Помимо обстоятельств, входящих в предмет доказывания в соответствии со ст.73 УПК РФ, при допросе у потерпевшего необходимо выяснить: где, когда, кем и как было обнаружено преступление; как долго длилось совершение преступления, каким способом и с использованием каких средств оно было совершено; в чем конкретно выразились последствия совершения преступления; каковы характер и размеры вреда, причиненного преступлением; предмет преступления и его размеры; кому могут быть известны сведения об обстоятельствах совершения и обнаружения преступления или наступления последствий преступления; известны ли ему какие-либо сведения о лицах, совершивших преступление.

---

[1] Мобильный банкинг является разновидностью ннтернет-банкинга. Интернет-банкинг – (в том числе через WEB-сайт(ы) в сети «Интернет» и включающего информационное и операционное взаимодействие с ними) // Письмо Банка России от 31.03. 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем Интернет-банкинга».

[2] Кроме того, на официальном интернет-сайте банка, как правило, имеется соответствующая ссылка на такое приложение, пройдя по которой на мобильном устройстве, абонент автоматически попадает на страницу его загрузки.

Так, А. отправил на абонентский номер принадлежащий С. SMS-сообщение, содержащее заведомо ложные сведения о том, что ее банковская карта заблокирована. Получив сообщение, С. перезвонила на абонентский номер А., который, представившись по телефону сотрудником Сбербанка России, подтвердил информацию о блокировке банковской карты и пояснил, что необходимо произвести «перезагрузку» банковской карты. Для этого он убедил С. совершить у банковского терминала с использованием ее банковской карты ряд действий, в результате которых с ее счета были похищены денежные средства в размере 29 754 руб. [2].

В ходе допроса потерпевшего необходимо детально выяснить, каким конкретно мобильным средством связи он пользуется, какие программы, как и при каких обстоятельствах им (или иными лицами) были установлены на мобильное устройство, какой операционной системой управляется данное мобильное устройство, как часто он использует данное мобильное устройство, имеет ли данное устройство программы, позволяющие защищать данные, хранящиеся на данном устройстве, вносились ли изменения в операционную среду данного устройства, кем и при каких обстоятельствах и пр.

Кроме того, необходимо детально установить наличие принадлежащего потерпевшему банковского счета, банковской карты, соответствующего программного обеспечения (Мобильного банкинга), установленного на мобильное устройство, позволяющего управлять средствами, расположенными на банковском счете (банковской карте).

Выяснить пароль доступа к программному обеспечению «Мобильного банкинга», определить степень его сложности, установить меры сохранности данного пароля для третьих лиц, предпринимаемые потерпевшим [5].

В случае, если потерпевший и преступник использовали для общения SMS-сообщения, необходимо подробно отразить содержание каждого из них, отдельно уделяется внимание отражению в протоколе признаков речи, если происходило голосовое общение – речевых дефектов (картавость, шепелявость и пр.), использование слов паразитов, специальных слов и терминов – технических, из банковской сферы, а также слов и словосочетаний, носящих ярко выраженный, индивидуальный характер, позволяющих в дальнейшем дополнительно идентифицировать лицо по этим признакам (темп речи, манера говорить, голос). Необходимо точно отразить в протоколе детали разговора с мошенником, отразить точную дату и время совершения абонентских соединений, отправки SMS и пр.

Допрос свидетелей. В качестве свидетелей по уголовным делам данной категории, как правило, допрашиваются сотрудники банка (кредитной организации), представители оператора мобильной связи, лица, выявившие преступление, а также иные лица, которым известны определенные обстоятельства совершения преступления или сведения, характеризующие личность подозреваемого, обвиняемого.

У свидетелей – сотрудников банка (кредитной организации) необходимо выяснить:

– какие банковские продукты имеются в банке (карты (счета)), какие карты (счета) были открыты в данном банке потерпевшим;

– особенности открытых счетов, порядок обслуживания и предоставления дополнительных услуг по счету[1];

– какое программное обеспечение используется и предоставляется держателю банковской карты для удаленного доступа и управления счетом;

– кто является разработчиком данного программного обеспечения;

– какие операции возможно совершить, используя данное программное обеспечение;

– каков порядок установки и использования таких программ, каковы требования банка, предъявляемые к держателю карты, использующему интернет-банкинг и Мобильный банкинг;

– возможно ли внесение изменений в работу таких программ третьими лицами, что для этого требуется, и пр.;

– какими способами можно получить необходимую и достаточную информацию (какую именно) для совершения операций со счетом банковской карты потерпевшего;

– с какими операторами мобильных средств связи и в каких объемах заключены надлежащие договоры, в соответствии с которыми оператор связи предоставляет удаленный доступ в сеть «Интернет» по соответствующему защищенному каналу, используемые способы защиты таких каналов и пр. [4].

В качестве свидетеля (представителя мобильного оператора связи) можно допросить соответствующее лицо, имеющее доступ к сетям телекоммуникационной связи, компьютерной информации – системного администратора, который может дать показания относительно особенностей предоставления соответствующих услуг мобильной связи,

[1] Например, банк может установить определенные лимиты для держателя карты по снятию определенного количества денежных средств в сутки, определенные лимиты списания денежных средств при оплате покупок, когда не требуется вводить ПИН-код в платежном терминале, и пр.

включая особенности предоставления удаленного доступа к сети «Интернет» по выделенным (защищенным) каналам, для использования соответствующего программного обеспечения Мобильный банкинг и пр. [3].

Лица, выявившие преступление и установившие личность подозреваемого, обвиняемого (сотрудники оперативных подразделений органов, осуществляющих оперативно-разыскную деятельность, в должностные обязанности которых входит раскрытие преступлений в сфере компьютерной информации) также допрашиваются по обстоятельствам, ставшим им известным относительно совершенного преступления.

Свидетели могут быть допрошены также в целях получения сведений, характеризующих личность потерпевшего, подозреваемого, обвиняемого. Кроме того, доказательственную информацию можно получить при допросе по таким делам родственников потерпевшего, а также подозреваемого, обвиняемого.

Библиографический список

1. Власов П. Е. О законодательной регламентации некоторых следственных действий // Библиотека криминалиста. – 2016. – № 2. – С. 43–48.

2. Судебное решение Надымского городского суда ЯНАО по делу № 1-4/2014 (1-261/2013). ULR: http:// bsr.sudrf.ru (дата обращения: 13.06.2017).

3. Попов Д. О., Иванов В. Ю. Правовые основы проведения компьютерной технической экспертизы // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2014. – С. 116–122.

4. Васильева Е. А., Пузарин А. В., Захаров Д. Н. Исследование возможности применения биллинговых записей // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 52–55.

5. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2.

И. А. Гуляева[1], ***В. В. Гончар***[2]

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПО ПРОИЗВОДСТВУ ОБЫСКА, СВЯЗАННОМУ С ИЗЪЯТИЕМ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Ежедневно человеком применяются различные технические средства в целях обмена информацией, фиксирования каких-либо событий окружающего мира. Вместе с тем, научно-технический прогресс несет в себе и опасность применения информации для достижения противоправной цели [1, с. 27].

Производство следственных действий в сфере такой категории преступлений отличается повышенной сложностью, поскольку осуществить их наличием специальных знаний – попросту невозможно.

В настоящее время алгоритм действий следователя по проведению обыска, связанного с изъятием электронных носителей информации, по мнению исследователя В. Б. Вехова [2, с. 2], недостаточно освещен в научных трудах и исследованиях. На практике к такому обыску привлекают несколько следственно-оперативных групп, подборка которых осуществляется следователем с учетом знания и накопленного опыта по проведению обыска на вычислительной технике.

Подготовка в проведении такого обыска включает в себя два основных этапа:

Во-первых, это проведение действий до выезда на место происшествия.

Для этого следователю необходимо получить информацию об имеющейся вычислительной технике в помещении, где будет происходить обыск, по возможности – о ее количестве.

Во-вторых, проведение конкретных действий на месте происшествия. Следователю необходимо выяснить, подключены ли к вычислительной технике блоки бесперебойного питания. Это важно знать, поскольку от их наличия зависит, возможно ли уничтожение информации подозреваемыми лицами на вычислительной технике в случае отключения электроэнергии.

По прибытии на место следователю и следственно-оперативной группе необходимо молниеносно войти в помещение, чтобы предот-

---

[1] Курсант 406 учебного взвода 4 В курса Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Гуляева И. А., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

вратить уничтожение информации, а также пригласить понятых до предъявления постановления о производстве обыска, т. к. начинать обыск можно только после приглашения понятых. Весьма эффективным будет для следователя дать поручение участникам следственно-оперативной группы охранять вычислительную технику и не подпускать к ней лиц, находящихся в обыскиваемом помещении.

Однако дополнительно необходимо следующее: выполнить требование ч. 9.1 ст. 182 УПК РФ, а именно: пригласить специалиста.

Сам факт отсутствия специалиста в процессе обыска и изъятия информации с электронных носителей является основанием для признания такого обыска незаконным. Впоследствии это может обернуться основанием для отмены приговора по делу.

Так, адвокатом М. В. Спиридоновым была в 2016 г. опубликована статья, в которой он поделился практическим опытом: «Доводы жалобы в части отсутствия специалиста при изъятии электронных носителей информации были приняты во внимание прокурором, в результате чего жалоба была частично удовлетворена, обыск был признан незаконным, на имя руководителя следственного органа было вынесено соответствующее представление, результатом которого стало признание недопустимыми доказательствами предметов (электронных носителей информации) изъятых в ходе указанного обыска» [3, с. 5].

Необходимо также подготовить технические устройства, с помощью которых изъятая информация будет считана и хранима. Следователю необходимо установить личность гражданина, которому принадлежит вычислительная техника, подлежащая обыску. Требуется также установить время проведения обыска. По мнению исследователя Худякова, наилучшее время для проведения обыска электронных носителей – утренние часы нерабочего времени [4, с. 45].

В случае, если вычислительная техника установлена не в одном, а в нескольких помещениях, то обыск необходимо проводить одновременно во всех этих помещениях.

В процессе проведения инструктажа для следственно-оперативной группы следователь должен обратить внимание всех ее участников на том какое конкретно преступление расследуется, какие документы или предметы необходимо найти и изъять, каким образом следует обращаться с вычислительной техникой.

Также необходимо помнить, что следователю на этапе подготовки проведения обыска нужно определить вид компьютерной среды, который можно разделить на автономный (то есть, работающий в незави-

симости от другой вычислительной техники) и сетевой (то есть, имеющий общий канал обмена базой данных). Зачастую возникает сложность в отслеживании всех сопряженных в единую сеть компьютеров, а также в поиске места расположения запоминающего устройства [11].

Непосредственно на месте происшествия следователю необходимо зафиксировать все действия, которые производятся, а также полученные результаты. После чего важно позаботиться о транспортировке вычислительной техники.

Можно выделить два способа изъятия информации с вычислительной техники: одновременно с носителем информации либо без него.

Изъятие информации вместе с носителем предполагает изъятие собственно носителя информации или системы устройств. Этот способ считается наиболее приемлемым, поскольку позволяет выявить какие-либо другие доказательства. Второй способ изъятия информации является более сложным, поскольку процесс изъятия информации в разрыве с общей информационной базой влечет частичную утерю изымаемых данных либо их изъятию не в полном объеме.

По мнению исследователей И. С. Федотова, П. Г. Смагина, в процессе изъятия вычислительной техники, необходимо обращать внимание на пароли и коды, осмотр документов; изъять все материалы, компьютеры и магнитные носители [5, с. 194].

В настоящее время в практике распространены случаи производства обыска с электронных носителей информации до возбуждения уголовного дела. Это связано с тем, что предварительная проверка, проводимая органами следствия, проводится в сроки, установленные законодательством [6, с. 9].

В соответствии с положениями Федерального закона от 4 марта 2013 г. № 23-ФЗ «О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации» значительно расширены процессуальные возможности сотрудников органов предварительного расследования [7, с. 117].

С учетом законодательных изменений представляется возможным предложить следующие позиции, которые должны быть отражены в плане доследственной проверки по делам о преступлениях в сфере компьютерной информации:

– получение письменного объяснения от заявителя;

– осмотр места происшествия – места обнаружения следов преступления с обязательным осмотром электронно-вычислительной машины или иного компьютерного устройства, электронных носителей и содержащейся на них компьютерной информации;

– получение письменных объяснений у лиц, на которых ссылается заявитель или имеются данные о них как о возможных свидетелях происшедшего события;

– ознакомление с технологией использования документированной компьютерной информации в конкретном технологическом процессе или операции [8, с. 119].

Борьба с преступлениями в сфере компьютерной информации должна оставаться одной из приоритетных задач для правоохранительных органов, обеспечивающих общественную безопасность Российской Федерации. В противном случае нарастание негативных процессов, протекающих в общественной среде нашего государства, создаст угрозу национальной безопасности России [9, с. 134], [10, с. 18].

Библиографический список

1. Гончар В. В. Теоретические и правовые аспекты разыскной деятельности следователя: монография. – М. : Инфра-М, 2017.
2. Вехов В. Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // СПС «КонсультантПлюс». (дата обращения: 15.01.2018).
3. https://адвокат-спиридонов.рф/изъятие-электронных-носителей/.
4. Худяков А. А. Особенности производства следственных действий при расследовании преступлений в сфере компьютерной информации. – М., 2013.
5. Федотов И. С., Смагин П. Г. Электронные носители информации: «вещественные доказательства» или «иные документы» // Вестник Воронежского государственного университета. Серия «Право». – 2014. – № 3.
6. Калиновский С. Б. «Доследственный» обыск – незаконное ноу-хау // Уголовный процесс. – 2015. – № 1.
7. Ермаков С. В., Макаренко М. М. Отдельные поводы и основание для возбуждения уголовных дел о преступлениях в сфере предпринимательской и иной экономической деятельности // Вестник экономической безопасности. – 2017. – № 1. – С. 116–121.
8. Орлова А. А., Гончар В. В., Батюк В. И., Мешков М. В. и др. Предварительное следствие в органах внутренних дел : учебное пособие / под ред. М.В. Мешкова. – М. : Щит-М, 2007.

9. Гончар В.В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

10. Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. – 2017. – № 10. – С. 18.

11. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел : сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.

***Е. С. Юрченкова*[1], *В. В. Гончар*[2]**

НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

В настоящее время больше количество людей в мире используют пластиковые карты, оплачивают с помощью их счета и проводят различные операции. Существует множество видов пластиковых карт – дебетовые, кредитные, игровые, премиальные, доходные, подарочные (предоплаченные). Каждая из них обладает различными уровнями защиты. По уровню защиты разделяют магнитные и чиповые, которые надежнее и безопаснее, электронный микропроцессор (чип) имеет более сложный алгоритм защиты, карты с магнитной полосой легко подделать. В России банки выпускают в основном комбинированные карты: и с чипом и с магнитной лентой. Если в торговой точке будет устаревший платежный терминал, который не обслуживает чиповые карты, можно будет произвести оплату с помощью магнитной полосы. Постепенно чиповые карты полностью вытеснят карты с магнитной полосой как в России, так и в других странах. В последнее время увеличивается выпуск банковских карт с бесконтактной технологией оплаты – MasterCard PayPass и Visa payWave. На них изображен значок в виде волн. Бесконтактные карты позволяют экономить время и рас-

[1] Курсант 4 Л курса Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Юрченкова Е. С., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

плачиваться за покупки не вводя ПИН-код (если сумма покупки меньше 1 тыс. руб.), прикладывая карту к платежному терминалу.

Стоит отметить, что первой платежной системой является Diners Club, созданная в 1950 г. Однако точкой отсчета развития системы коммерческих банков следует считать принятие Закона «О банках и банковской деятельности» в 1990 г., который закрепляет основные положения данного вида преступления. Хотя первые карты и появились относительно давно, их уровень защиты находится на должном уровне, с их использованием совершается множество преступлений, для пресечения которых необходимо уделять особое внимание не только методам расследования данных видов преступлений, но и их профилактике. Такие преступления можно объединить в следующие группы:

– злоупотребления с подлинными банковскими картами;

– изготовление поддельных банковских карт;

– сбыт поддельных банковских карт;

– использование поддельных банковских карт.

Так, рассматривая первую категорию преступлений, стоит отметить, что 1 января 2014 г. вступила в силу новая редакция девятой статьи ФЗ «О национальной платежной системе», в соответствии с которой ответственными за несанкционированное списание денег со счета клиента являются банки-эмитенты. В связи с этим появляется возможность совершения преступных действий недобросовестными пользователями, так как клиент может потратить денежные средства с карты, далее сообщить в течение суток после проведения операции, что денежные средства были списаны без пользовательского согласия. При расследовании данного вида преступления стоит обратить внимание на установление следующих обстоятельств:

– время, место, способ совершения транзакции. Если в ходе проведения проверки будут установлены события, противоречащие заявлению, то в возбуждении уголовного дела за отсутствием события преступления будет отказано;

– характер и размер причиненного ущерба. Для этого необходимо получить у банка-эмитента информацию о состоянии лицевого счета, с которого были списаны денежные средства. Установление определенной суммы необходимо для отграничения уголовного правонарушения от административного;

– вид списания денежных средств: получение наличных денежных средств в банкомате, оплата какого-либо товара и т. п.;

– потерпевший, которому причинен ущерб. Данное обстоятельство необходимо для установления лица, проводящего транзакцию;

– характеристика банковской карты и ее связь с пострадавшим лицом (с этой целью в банке-эмитенте выясняется: действительно ли банковская карта с соответствующими реквизитами эмитировалась ранее; тип банковской карты; срок ее действия; кому и когда она была выдана; выпускались ли дополнительные банковские карты);

– сведения о том, что были ли известны реквизиты и ПИН-код соответствующей карты другим.

В рамках проверки сообщения о совершении кражи или мошенничества могут быть установлены следующие факты: возможно ли совершение транзакции держателем банковской карты, если он в силу объективных обстоятельств об этом не помнит из-за сильного алкогольного опьянения либо расстройства памяти. Также транзакция могла быть совершена родственниками, либо близкими лицами. Данное обстоятельство примечательно тем, что даже в ситуации, когда транзакция совершена против воли держателя карты его близким лицом, держатель карты подает ходатайство о прекращении уголовного дела.

Результатом проведенной проверки может быть и отказ в возбуждении уголовного дела ввиду того, что держатель может быть не осведомлен о комиссии при снятии денежных средств либо заблуждаться в их количестве на лицевом счете, либо банковская карта может быть захвачена банкоматом. В том случае, если будет получена информация, подтверждающая факт кражи или мошенничества, в ответе будет содержаться информация о времени, месте, сумме, проводимой операции. Стоит также отметить, что ввиду того, что каждому платежному терминалу в системе проведения транзакций присвоен личный номер, имеется регистрация по месту его нахождения, уже в процессе авторизации можно определить место посылаемого запроса – конкретное помещение или участок местности, оборудованные банкоматом или POS-терминалом. По операциям, совершаемым с использованием Интернета, установление места совершения преступления, направляя запрос в банк, не представляется возможным, т. к. в данных случаях использование платежных терминалов не происходит, либо информация с магнитной полосы или чипа не считывается. Сведения об использованных при совершении хищения реквизитах банковских карт могут остаться в интернет-магазине, банке, где открыт расчетный счет у интернет-магазина, в процессинговом центре, а также в банке-эмитенте, куда направлялся авторизационный запрос на проведение транзакции.

Интересующие должностное лицо данные об особенностях интернет-соединения пользователя с интернет-магазином по запросу могут быть предоставлены провайдером. Органам внутренних дел о кражах и мошенничествах, совершенных с использованием банковских карт и их реквизитов, становится известно, как правило, в ходе осуществления оперативно-разыскной деятельности. В этой ситуации следователь должен правильно выбрать момент реализации оперативных материалов, учитывая, что уголовная ответственность наступает «только за приготовление к тяжкому и особо тяжкому преступлению» [1, ч. 1 ст.30]. Сложность вызывает доказывание умысла на совершение кражи или мошенничества в крупном размере на стадии подготовки, организованный характер преступной группы. Кроме того, задержание преступников на стадии подготовки их к совершению хищений может привести к тому, что возбужденное уголовное дело будет прекращено за отсутствием в деянии состава преступления. В целях увеличения эффективности проводимой проверки до возбуждения уголовного дела были проведены оперативно-розыскные мероприятия для уточнения численного состава преступной группы, а также преступных замыслов ее членов, а именно: опрос, наведение справок, наблюдение, прослушивание телефонных переговоров, оперативное внедрение. Для обеспечения мониторинга транзакций в режиме реального времени необходимо «привлечь сотрудников банков с обязательным предупреждением их о неразглашении условий подобного сотрудничества» [2, с. 23].

Подводя итог, хотелось бы отметить, что на современном этапе развития общества существует ряд проблем при расследовании преступлений, совершаемых с использованием платежных карт, уровень правового и организационного обеспечения их раскрытия, расследования и предупреждения требуют совершенствования [3, с. 123].

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 31.12.2017) // СПС «КонсультантПлюс» (дата обращения: 29.01.2018).

2. Малокостов В. О. преступности в области пластиковых карточек // Мир карточек. – 1999. – № 12.

3. Орлова А. А., Гончар В. В., Батюк В. И., Мешков М. В. и др. Предварительное следствие в органах внутренних дел: учебное пособие / под ред. М. В. Мешкова. – М. : Щит-М, 2007.

Н. Д. Тютлина[1], *В. В. Гончар*[2]

АКТУАЛЬНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ НЕЗАКОННОГО ОБНАЛИЧИВАНИЯ ДЕНЕЖНЫХ СРЕДСТВ ЧЕРЕЗ КРИПТОВАЛЮТУ

В настоящее время весьма актуальной является проблема незаконного обналичивания денежных средств. Негативные социально-экономические, а также правовые последствия данного явления пагубно отражаются как на российской экономике, так и на уровне правопорядка в нашем обществе. В целом незаконное обналичивание денежных средств можно обозначить как вид незаконной экономической деятельности и негативное социальное явление; а также действия, совершаемые хозяйствующими субъектами (юридическими лицами и индивидуальными предпринимателями) в целях уклонения от уплаты налогов и получения наличных денежных средств, не отраженных в официальных бухгалтерских документах хозяйствующего субъекта.

Следовательно, обналичивание подразумевает «получение организацией наличных денег, дальнейшее распоряжение которыми не могут проследить контролирующие органы. Получающийся в результате этого процесса «черный нал» позволяет организации рассчитываться по хозяйственным операциям и выплачивать зарплату, одновременно уклоняясь от уплаты налогов, реальные руководители организаций могут использовать его для личного обогащения, дачи взяток, коммерческих подкупов [1].

Согласно ст. 75 Конституции Российской Федерации денежной единицей в Российской Федерации является рубль. Эмиссия денежных средств осуществляется исключительно Центральным Банком России. Между тем век высоких технологий коснулся всех сфер жизнедеятельности человека.

Криптовалюта – это особое электронное платежное средство, курс которого поддерживается только спросом и предложением, при использовании которого отсутствует централизованный администратор, а также контроль со стороны государственных органов. При создании этой валюты используется особый криптографический шифр, состоя-

---

[1] Слушатель 506 учебного взвода факультета подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Тютлина Н. Д., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

щий из последовательного хеширования и цифровой подписи. Говоря простым языком, это цифровая валюта, в качестве ее единицы выступают монеты (coin). Они защищаются от возможности подделки, представляя собой зашифрованную информацию, недоступную к копированию, благодаря использованию метода криптографии. Каждая криптоединица представляет собой последовательность блоков, а каждый из блоков – сложную математическую формулу. Для создания новой монеты необходимо сгенерировать новую цепочку блоков транзакций. Воспроизводство криптографических валют не зависит от стран, правительств и международных взаимоотношений. На курс криптовалюты относительно других валют влияет только сложность их создания, производства («майнинга») и спрос на нее для совершения взаиморасчетов [2]. Эмиссию криптовалюты способен осуществить практически каждый программист. На сегодняшний день на рынке существует более 700 видов криптовалюты с различным курсом и количеством монет. Основной из них является криптовалюта «bitcoin» – Биткоин. В основе биткоина лежит публичный реестр («Blockchain» или «цепочка блоков») – блокчейн, в котором хранится информация обо всех произведенных транзакциях, то есть платежных операциях пользователей. Таким образом, «блокчейн» – это база данных, которая хранится одновременно на множестве компьютеров. Новые блоки в этой базе-цепочке создаются постоянно. Каждый вновь созданный блок содержит группу накопленных за последнее время и упорядоченных записей (транзакций), а также заголовок.

Обменять биткоины на наличные деньги проще всего через интернет-ресурсы. Чаще всего используются следующие способы:

Биржи. Многие криптовалютные биржи предоставляют услугу по выводу виртуальных денег. Для этого необходимо зарегистрироваться на бирже и перевести средства на свой биржевой счет. За совершение обменной операции биржи берут комиссию. Размер комиссии каждая биржа устанавливает самостоятельно, так же как и способы вывода средств (WebMoney, Яндекс Деньги, банковский перевод и т. д.). Для совершения некоторых действий пользователю придется пройти верификацию: предоставить удостоверение личности и документы, подтверждающие адрес. Как правило, верификация необходима для вывода крупных сумм (от 1 биткоина) или для использования определенных способов перевода (вывод на банковский счет). Среди крупных русскоязычных бирж можно назвать EXMO, LiveCoin. Этот вариант подходит тем, кто собирается вывести большой объем средств.

Многие биржи предлагают разные варианты вывода, поддержку и простоту перевода. С другой стороны, клиенты биржи не застрахованы от хакерских атак и мошеннических действий со стороны руководства площадки [3].

Платежная система WebMoney. С недавнего времени в этой системе появился кошелек WMX, являющийся аналогом биткоина. Данный кошелек можно пополнять, например, через основной bitcoin-кошелек. Для этого необходимо создать в системе WMX кошелек и выбрать пункт «пополнить переводом Bitcoin», это перенаправит вас в специальную закрытую зону системы, вход в которую потребует повторной авторизации. Тут вы сможете узнать номер своего BTC кошелька для пополнения, которому также будет присвоен QR код. После пополнения можно обменять биткоины внутри системы на рубли и вывести их на привязанную к системе карту.

Выпуск платежной карты, имеющей привязку к биткоин-кошельку (Wirex, Xapo, AdvCash, BitPlastic, BitPay). При выпуске пластиковых карт можно выбрать различные платежные системы: Visa, Mastercard. Счет может быть в стандартной валюте и привязан к системе (в этом случае конвертация осуществляется при пополнении карты), а также в криптовалюте (конвертация происходит в момент использования карты при покупке товаров или услуг). В России такие карты пока не выпускают, а потому помимо стоимости изготовления карты (до 20 долларов), вам потребуется оплатить и доставку. Биткоин-картам присущи все недостатки стандартных банковских операций – комиссии, обязательные платежи за обслуживание, потеря на курсе валют [4].

Обмен через посредников. Существуют площадки, на которых физические лица ищут контрагентов и договариваются о сделке. Курс обмена стороны устанавливают самостоятельно. Одна из самых крупных площадок – LocalBitcoins.net. Этот вариант самый ненадежный, так как у продавца криптовалюты отсутствуют гарантии. Если покупатель окажется недобросовестным, деньги просто исчезнут [6, 7].

Однако не стоит забывать и о том, что продукты криптографии – биткоины, смарт-контракты – имеют и другую сторону, они провоцируют рост интернет-преступности. Примечательно, что одними из первых пользователей и владельцев криптовалюты как раз и стали преступники, для которых биткоин оказался удобной альтернативой традиционным деньгам для мошенничества на интернет-площадках. В силу отсутствия единого стандарта регулирования «цифровой валюты», каждая страна пока самостоятельно определяет, являются ли опе-

рации с биткоинами или любыми другими виртуальными деньгами нарушением местных законов. Основной формой противоправного использования криптовалют является отмывание с их помощью денег за незаконные виды деятельности, не редки случаи кражи криптовалюты с чужих счетов владельцев криптовалюты. Примером этого являются следующие преступления:

1. Газета «Ведомости» от 1 сентября 2017 г. сообщает, что в России возбуждено первое уголовное дело за обналичивание биткоинов. Костромские полицейские и сотрудники ФСБ задержали троих людей, которые нелегально зарабатывали на обналичивании и продаже биткоинов, сообщила представитель МВД Ирина Волк. Согласно сообщению МВД фигуранты дела незаконно обналичили более 500 млн руб. В отношении них возбудили дело по статье «Незаконная банковская деятельность», и сейчас они находятся под подпиской о невыезде. Чтобы обменивать и переводить криптовалюту, задержанные оформили на своих родственников более 300 банковских и sim-карт, говорится в сообщении МВД [5].

Каким же образом отмываются и обналичиваются биткоины? Некоторым пользователям SilkRoaded2 удалось отследить, как были выведены средства, а затем и какой способ незаконного получения криптовалюты использовал злоумышленник. Эту детективную историю описывает один из авторов разоблачения: «*Весь день я гонялся за негодяем с украденными биткоинами используя blockchain. Метафорически, я преследовал его, наблюдая сквозь стеклянную крышу движущегося поезда. Я отставал от него меньше чем на 20 минут, или на «два подтверждения сети». Вор отчаянно создавал новые адреса для кошельков и выводил через них средства из 49 изначальных бумажников, каждый раз ожидая трех или четырех подтверждений сети, прежде чем перевести средства снова. Каждый раз, когда я догонял его, я «шестьсот-шестьдесят-шестерил*» его – отправлял вдогонку на отловленные адреса по 0,00666 биткоинов, чтобы испортить его прекрасные круглые числа, типа 4000, или 8000. Затем внезапно стали появляться суммы с десятичными разрядами, и вот уже дробные биткоин-счета прыгают с кошелька на кошелек, как саранча на электрической плитке, совсем не останавливаясь для подтверждения. Теперь он смешивал и отмывал наши украденные биткоины второй раз, и этот «*миксер» – сервисы, которые позволяют пользователям скрыть происхождение своих биткоинов, был непобедим. Если вы, конечно, не угадаете, что конкретно за способ он использует, такой, в котором отмываются почти все отслеживае-*

мые средства, и не смешаете небольшую часть своих биткоинов вместе с ними, пропустив небольшое количество через те же кошельки и используя тот же алгоритм. Я прыгал с ноги на ногу с криками «давай!» на моем ноутбуке, сто лет ожидая шести подтверждений сети, чтобы провести 0,5 BTC в «Bitcoin Fog». Мой пол-биткоин был в итоге нашинкован и пропущен через огромное количество кошельков, и я последовал за самой большой порцией через blockchain.info и обнаружил адреса с нашими украденными 96 000 BTC!».

2. В Греции 25 июля 2017 г. задержали гражданина России Александра Винника по подозрению в «отмывании» $4 млрд через биткоины. Арестован россиянин был по запросу США, где ему заочно предъявлено обвинение. Он подозревается в причастности к организации крупной схемы легализации средств с помощью биткоин-биржи BTC-e, а также во многих других преступлениях. В пресс-релизе на сайте министерства юстиции США говорится, что Винник занимался преступной деятельностью как минимум с 2011 г., то есть с момента основания BTC-e. Он, утверждают следователи, воровал и использовал личные данные пользователей, был причастен к наркоторговле и помогал преступным группировкам отмывать деньги.

По версии обвинения россиянин отмывал деньги, которые были получены после хакерской атаки на японскую биржу криптовалют Mt. Gox. Тогда в 2014 г. из нее были похищены 850 тыс. биткоинов (около $500 млн. по курсу на момент похищения), из которых 306 тыс. выведены в связанные с BTC-e электронные кошельки.

Следует отметить, что для эффективного противодействия криминальному обороту криптовалюты международное сообщество должно разработать единую стратегию, реализуемую в следующих ключевых направлениях:

– определение юридической природы криптовалюты, позволяющее избавиться от коллизии при решении юрисдикционных вопросов. На международном уровне должен быть решен вопрос о том, чем же является криптовалюта: товаром, валютой, платежным инструментом, приравненным к некоторым видам ценных бумаг, средством накопления или формой платежной услуги. Ответ на данный вопрос позволит унифицировать юридическую практику во всех странах, поставив оборот криптовалюты на привычные правовые рельсы;

– установление универсальной юрисдикции государств в отношении преступников, осуществляющих отмывание денежных средств,

финансирование терроризма, оборот наркотиков и оружия с использованием криптовалюты;

– создание реестра проверок, обязательных при работе с финансовыми потоками из стран с неэффективными режимами борьбы с отмыванием преступных доходов и финансированием терроризма;

– расширение спектра информации, доступной подразделениям финансовой разведки, предоставлением им упрощенного доступа к информации о совершаемых действиях;

– распространение положений Директивы Европейского союза (ЕС) по борьбе с отмыванием денег и финансированием терроризма от 26 июня 2015 г. на использование криптовалют. В первую очередь это касается мер по надлежащей проверке клиента (МНПК).

Применительно к криптовалютам необходимо нормативно закрепить пять параметров легитимности транзакции в рамках предупреждения легализации преступных доходов: идентификация клиента (сбор данных), верификация на основе документов, данных и информации (проверка достоверности), определение бенефициарного собственника, оценка целей деловых отношений, мониторинг в соответствии с профилем риска.

Библиографический список

1. Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: http://www. eurasiangroup.org/ files/FATF_docs/Virtualnye_ valyuty_FATF_2014.pdf.

2. Вотинов М. В., Пайкачева К. В. Криптовалюта: сложности внедрения и использования // Вопросы экономики и управления. – 2017. – № 2. – С. 6–8.

3. Официальный сайт Bitcoin: [Электронный ресурс]: – Режим доступа – URL: http://bitcoin.org.

4. [Электронный ресурс]: – Режим доступа – URL: https://bloomchain.ru/ kak-obnalichit-kriptovalyutu-obzor-variantov.

5. Первое уголовное дело за обналичивание биткоинов заведено в России // Ведомости. – 2017. – 1 сентября.

6. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (т. 2).

7. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – № 2 (20). – С. 30–38.

Н. К. Рудакова[1], *В. В. Боровикова* [2]

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ст. 110[2] УК РФ

26 августа 2017 г. вступила в законную силу новая ст. 110[2] УК РФ, предусматривающая уголовную ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства. Официально зафиксировано Следственным комитетом Российской Федерации детских самоубийств в связи с участием в сообществах суицидальной направленности в 2014 г. около 400, 2015 г. – 504, 2016 г. – 720, в 2017 г. – более 2300.

По данным Российского агентства правовой и судебной информации (РАПСИ) по ст. 110 УК РФ в 2014 г. было возбуждено 26606 уголовных дел, осуждено – восемь человек; в 2015 г. возбуждено 25476 уголовных дел, осуждено – 15 человек; в 2016 г. – 22800, осуждено – 16 человек. На октябрь 2017 г. возбуждено 3000 уголовных дел, более 930 из которых в отношении администраторов и кураторов сообществ суицидальной направленности. Проанализировав статистику последних лет, можно с уверенностью сказать, что тенденция возрастает. Также существует повышенная общественная опасность в связи с организацией деятельности, направленной на побуждение к совершению самоубийства несовершеннолетними лицами.

Социальная обусловленность уголовного запрета, предусмотренного ст. 110.2 УК РФ, определяется следующими обстоятельствами: общественная опасность доведения до самоубийства очевидна, т. к. потерпевший может лишиться самого дорогого, что у него есть, т. е. жизни. Тем более, повышенную опасность представляют случаи, если эта деятельность приобретает организационные начала, чему способствует широкое распространение среди населения России Интернета. Организаторы одновременно могут повлиять на сознание тысяч пользователей интернета. О негативных последствиях такого рода воздействия можно вести речь только используя самые большие цифры.

Необходимо иметь в виду, что среда, в которой распространяются призывы к совершению самоубийства, как правило, молодежная (немало среди этой молодежи и несовершеннолетних). Вред от такого распространения для формирования личности также велик. Даже если подобные призывы не найдут своего отклика среди молодежной ауди-

---

[1] Курсант 232 учебного взвода 2 И курса факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Рудакова Н. К., 2018.

[2] Доцент кафедры уголовного права МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Боровикова В. В., 2018.

тории, все равно это отрицательно оказывает воздействие на формирование личности, прежде всего несовершеннолетних. Поэтому государство должно реагировать самыми жесткими мерами на случаи организационной деятельности, направленной на побуждение к совершению самоубийства. Нельзя забывать, что вред от анализируемой деятельности причиняется и семьям потерпевших. Страдания, которые могут испытать родители и другие близкие родственники погибших, не поддаются исчислению. Это жизненная катастрофа, которую ничем нельзя исправить. Этот факт тоже «работает» в пользу установления уголовной ответственности за организацию деятельности, направленной на побуждение к совершению самоубийства.

Распространение идей суицида среди массовой аудитории дезорганизует людей, делает их зависимыми от различных форм негативного воздействия. В конечном счете, общество становится менее сплоченным, стойким к различного рода идеологическим диверсиям, которые осуществляют враги Российского государства.

Приведенные выше аргументы, на наш взгляд, подтверждают правильность установления уголовной ответственности за преступления, предусмотренные ст. 110.2 УК РФ. Одной из проблем по ст. 110^2 УК РФ является сбор судебной и следственной практики. На данный момент в период июля и октября 2017 г. в Российской Федерации возбуждено три уголовных дела в отношении кураторов смертельных сообществ по ст. 110^1 УК РФ и ст. 110^2 УК РФ. Например, в Подмосковье задержан 21-летний администратор группы «ВКонтакте», созданной в январе этого года, которая «склоняла подростков к совершению самоубийств». У группы было всего несколько десятков подписчиков, для которых задержанный придумывал «различные задания с целью оказать на них определенное психологическое воздействие».

Объектом посягательства по ст. 110^2 УК РФ является жизнь человека. Объективная сторона преступления, квалифицируемого в соответствии с ч. 1 ст. 110^2 УК РФ, состоит в организации деятельности, направленной на побуждение к совершению самоубийства с помощью распространения различной информации о способах совершения суицида или призывов к его совершению.

При расследовании преступления, квалифицируемого по ст. 110^2 УК РФ, важно выяснить следующий факт: преступное деяние является обособленным или звеном в системе организованной деятельности, направленной на побуждение к совершению самоубийства. Если преступление все же является звеном системы организованной деятельности, то благодаря выявлению данных о его мотивах и способах совер-

шения можно понять весь механизм действия как системы в целом, так и ее частей, то есть иных преступных деяний, входящих в ее цели. Увеличение масштабов организационной деятельности связано напрямую с привлечением в нее большого количества субъектов, как правило, организованных групп, специализирующихся на определенном виде преступления. Важно заметить, что законодатель в ст. 110^2 УК РФ не учел должным образом это обстоятельство. Поэтому полезно дополнить содержание ст. 110^2 УК РФ пунктом, содержащим квалифицирующий признак преступления, а именно: совершение данного преступного деяния группой лиц по предварительному сговору или организованной группой. Уголовная ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства, предусмотрена ст. 110^2 УК РФ, обусловлена тем, что данное деяние – это преступление особого рода. В нем последствия наступают непосредственно в результате действий самого потерпевшего, который вынуждается виновным к самоубийству. Именно анализ действий потерпевшего позволяет выяснить, намерен ли он был совершить самоубийство. При незавершенном самоубийстве анализ действий потерпевшего позволяет отграничить самоубийство от убийства.

Наступление опасных последствий часто связано с необдуманным поведением самих потерпевших, наличием семейных проблем, возрастными особенностями психики подростков, но, тем не менее, нельзя оставлять без внимания наличие злого умысла у организаторов и разработчиков подобного рода развлечений. Разработка таких игр основана на знаниях особенностей психологии подростков, технологий влияния на человека и, несомненно, носит социально-деструктивный общественно опасный характер. Таким образом, деяние «организация деятельности, направленной на побуждение к совершению самоубийства» выражает значительный уровень проявления общественной опасности и требует борьбу с ней необходимыми уголовно-правовыми нормами. В зарубежном уголовном законодательстве ряда государств имеются аналогичные российскому уголовному законодательству нормы об уголовной ответственности за доведение до самоубийства. Таким образом, проведенное исследование современного уголовного законодательства зарубежных стран выявило тот факт, что зарубежное законодательство имеет сходство с российским уголовным законодательством, как по конструкции состава преступления, так и по ряду последствий совершенных деяний и некоторым квалифицирующим признакам. Уголовная ответственность за доведение до самоубийства предусмотрена УК РФ в отношении вменяемого лица, достигшего 16-

летнего возраста. При том, что минимальный возраст самоубийства – 14 лет, то следует признать возраст лица, которое довело до самоубийства или организовало деятельность, направленную на побуждение в совершению самоубийства, также равным 14 лет и старше. На наш взгляд, изменение данного положения на законодательном уровне повысит эффективность суицид-превентивной деятельности в сфере применения уголовного закона. Представляется, что решить данную проблему необходимо следующим образом: ч. 2 ст. 20 УК РФ, регламентирующей возраст, с которого наступает уголовная ответственность, после слов: «. за убийство (ст. 105 УК РФ)» дополнить словами «за доведение до самоубийства (ст. 110 УК РФ)» и «за организацию деятельности, направленной на побуждение в совершению самоубийства (ст. 110^2 УК РФ)».

В примечании ст. 110^2 УК РФ сказано о том, что если виновное лицо, которое совершило преступление, квалифицируемое в соответствии со ст. 110^2 УК РФ, добровольно прекратило свою преступную деятельность и способствовало пресечению деяний, которые предусмотрены ст.ст. 110 и 110^1 УК РФ, освобождается от уголовной ответственности, если в его действиях не находится иного состава преступления. Само по себе наличие такого примечания стимулирует лиц, совершивших анализируемые преступления, к исправлению негативных последствий своего общественно опасного поведения. Вместе с тем, надо обратить внимание на то, что закон требует соблюдения двух условий освобождения от уголовной ответственности указанного лица. Необходимо наличие не только факта добровольного прекращения соответствующей преступной деятельности, но и обязательного при этом активного способствования раскрытию и (или) пресечению преступлений, предусмотренных ст.ст. 110, 110.1, 110.2 УК РФ. В противном случае такое освобождение исключается (т. е. одного добровольного прекращения здесь недостаточно). Кроме того, закон требует для полного освобождения от уголовной ответственности наличия того, что в действиях данного лица не должно содержаться иного состава преступления. Таким образом, есть резервы у правоприменителя для применения ст. 110^2 УК РФ.

Библиографический список

1. Собр. законодательства Рос. Федерации. – 2017. – № 24, ст. 3489.
2. Следственный комитет Российской Федерации. http://sledcom.ru/.

А. Л. Прохоров[1], *В. В. Гончар*[2]

ДЕЯТЕЛЬНОСТЬ СЛЕДОВАТЕЛЯ ПО ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИИ ИЗ БОРТОВОГО КОМПЬЮТЕРА АВТОМОБИЛЯ ПРИ РАССЛЕДОВАНИИ ДОРОЖНО-ТРАНСПОРТНЫХ ПРЕСТУПЛЕНИЙ

Дорожно-транспортное происшествие – событие, возникшее в процессе движения по дороге транспортного средства и с его участием, при котором погибли или ранены люди, повреждены транспортные средства, сооружения, грузы либо причинен иной материальный ущерб. Глава VI Федерального Закона от 10 декабря 1995 г. № 196-ФЗ «О безопасности дорожного движения» закрепляет ответственность за нарушение законодательства Российской Федерации о безопасности дорожного движения.

Расследование дорожно-транспортных преступлений прежде всего представляет собой определенную специфику в деятельности следователя и правоохранительных органов в целом. Это связано с быстро изменяющейся обстановкой, кратковременностью события, повышенной опасностью при работе на транспортной инфраструктуре и рядом других факторов. Сегодня на помощь приходят современные технологии и разработки. В частности, хотелось бы отметить возможности компьютерных систем автомобиля. Необходимость использования данных с данного вида устройств обусловлена зачастую недостаточностью доказательственной базы [3].

Бортовой компьютер в автомобиле может представлять ряд его функций. Это дает широкие возможности для получения данных, представляющих интерес при осуществлении предварительного расследования. Современные бортовые компьютеры обладают интегрированным модулем глобальной спутниковой навигации. Еще одной важной особенностью развития техники на рынке европейских и американских автомобилей в люксовых комплектациях стало появление дополнительного модуля долгосрочного хранения информации «черного ящика». В отличие от более ранних версий бортовых компьютеров, на котором сохраняется небольшой промежуток времени, то с по-

---

[1] Слушатель 5 В курса Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Прохоров А. Л., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

явлением «Черного ящика» информация представляет собой полную картину об автомобиле с самого ее выпуска с конвейера (рис. 1).

Рис. 1. Пример устройства вывода информации из бортового компьютера

При наличии в автомобиле бортового компьютера в целях всестороннего и полного объема доказательств необходимо назначать радиотехническую экспертизу. Целью, которой является изучение и исследование технического состояния, работы, выявление причин и причинно-следственных связей неполадок технического оборудования и систем.

В каждом конкретном случае из бортового компьютера данная экспертиза предоставляет возможность получить новые сведения по расследуемому преступлению, например, подтвердить или опровергнуть техническую неисправность автомобиля имеющуюся на момент ДТП.

2 можно более детально изучить перечень сведений, которые возможно получить после проведения радиотехнической экспертизы: от датчика ABS – состояние тормозной системы, применения торможения; от датчика рулевого управления – применение маневра; от GPS – расположение автомобиля и скорость движения; от датчика давления в шинах – состояние колес автомобиля перед и в момент ДТП; по показаниям спидометра – скорость движения; от датчика положения заслонки – увеличение скорости и крутящий момент.

Радиотехническая экспертиза позволит определить: технические характеристики и их назначение; исправна или нет тормозная система, световые приборы; скорость движения на определенном участке пути; режим работы коробки передач; исправна или нет электросистема; время нахождения в пути; было ли применение экстренного торможения.

Такой вид доказательства представляет важную роль при расследовании дорожно-транспортных преступлений [1, с. 50]. Данные, полученные после проведения радиотехнической экспертизы, наиболее точно раскрывают обстоятельства дорожно-транспортного происшествия. Это может повлиять на ход предварительного расследования в корне в таких случаях, когда имеются противоречия в показаниях участников дела, сопровождающиеся недостаточностью доказательственной базы. Ярким примером будет служить массовое дорожно-транспортное происшествие, в обстоятельствах которого достаточно сложно установить дорожную обстановку до момента происшествия.

Рис. 2. Наглядный пример технической возможности бортового компьютера (неисчерпывающий перечень зависит от комплектации)

Данные о применении торможения, совершения маневра, скорости движения также будут представлять интерес при дальнейшем проведении автотехнической экспертизы. В свою очередь точность и правильность предоставленных данных на автотехническую экспертизу в последующем позволит установить, имел ли водитель техническую

возможность предотвращения дорожно-транспортного происшествия, что, несомненно, представляет важную роль в повышении эффективности предварительного расследования и принятие законного и обоснованного решения.

По сведениям из открытых источников, в 2017 г. по всей России было менее десяти экспертов, способных на должном уровне проводить радиотехническую экспертизу.

Совершенно очевидно, что необходимо организовать подготовку большего количества таких экспертов, а данный метод надо использовать чаще, экспертизу назначать во всех случаях, если автомобиль оборудован бортовым компьютером, и до принятия решения об отказе в возбуждении уголовного дела либо его прекращения. На сегодняшний день бортовым компьютером оборудованы порядка более 70 % автомобилей, включая отечественного производства, и их количество будет увеличиваться [2, с. 135].

Библиографический список

1. Орлова А. А., Гончар В. В., Батюк В. И., Мешков М. В. и др. Предварительное следствие в органах внутренних дел: учебное пособие / под ред. М. В. Мешкова. – М. : Щит-М, 2007.

2. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 135.

3. Галиев Д. В., Пузарин А. В., Захаров Д. Н. Инструментальные средства добывания компьютерной информации, используемые для получения доказательств // Технологии информационной безопасности в деятельности органов внутренних дел Сборник научных трудов XIII научно-практической конференции. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 37–40.

Я. С. Городецкая[1], *В. В. Гончар* [2]

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В СВЯЗИ С ПРИНЯТИЕМ ПОСТАНОВЛЕНИЯ ПЛЕНУМА ВЕРХОВНОГО СУДА РФ ОТ 30 НОЯБРЯ 2017 г. № 48 «О СУДЕБНОЙ ПРАКТИКЕ ПО ДЕЛАМ О МОШЕННИЧЕСТВЕ, ПРИСВОЕНИИ И РАСТРАТЕ»

Новое Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. представляет собой объемный документ, состоящий из 35 пунктов. В нем впервые обращено внимание на квалификацию недавно выделенного вида мошенничества по ст. 159.6 УК РФ. Данное деяние было криминализировано Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Вышеуказанный Федеральный закон был принят уже после Постановления Пленума ВС РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате». Следовательно, уголовное законодательство сильно изменилось с момента появления предыдущего постановления. Поэтому определенность в толковании новых положений особенно значима.

Статье 159.6 УК РФ «Мошенничество в сфере компьютерной информации» присущи следующие особенности, отличающие ее от «простого» мошенничества. В первую очередь, данное преступление совершается совершенно иным способом, а именно: не путем обмана или злоупотребления доверием, а путем получения доступа к компьютерной системе и совершения ввода, удаления, блокирования или модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных

---

[1] Слушатель 506 учебного взвода Института подготовки сотрудников для органов предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Городецкая Я. С., 2018.

[2] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Гончар В. В., 2018.

сетей. В данном случае не происходит контакта человека с человеком, а указанные действия говорят о взаимосвязи человека с компьютером при помощи использования специально разработанных программ [2, с. 15]. Следующей особенностью является то, что по ст. 159.6 полностью отсутствует добровольная передача потерпевшим своего имущества преступнику. Хищение или приобретение права на чужое имущество совершается без ведома потерпевшего. Также в отличие от кражи изменяется смысл понятия «тайного способа», т. к. злоумышленник осуществляет вмешательство в компьютерную информацию пользователя, используя при этом его личную идентифицирующую информацию, чем нарушает безопасный порядок использования информационного пространства.

Согласно сведениям зонального информационного центра ГУ МВД России по г. Москва доля мошенничеств, совершенных в сфере компьютерной информации (ст. 159.6 УК РФ), от общего числа мошенничеств общеуголовной направленности (ст.ст.159-159.6 УК РФ) за девять месяцев 2017 г. составляет около 1,37 % (19 против 13828). В сравнении с аналогичным периодом 2016 года доля вышеуказанных преступлений (1,35 %) снизилась на 0,02 % (21 против 15536 преступлений).

Так, возвращаясь к статистике, за девять месяцев 2017 г. в г. Москва было предварительно расследовано 1744 мошенничеств общеуголовной направленности, из которых только 26 были квалифицированы по ст. 159.6 УК РФ, при этом раскрываемость данного вида преступлений составила 72,2 %. Для сравнения: за аналогичный период 2016 г. из 2324 предварительно расследованных мошенничеств общеуголовной направленности по ст. 159.6 УК РФ были квалифицированы только три преступления, раскрываемость составила 8,8 %.

Согласно статистических данных ГУ МВД России по г. Москва за девять месяцев 2017 г. было выявлено 17 преступников, которым было предъявлено обвинение по ст. 159.6 УК РФ, в 2016 г. таки преступников было выявлено лишь шесть.

Из нового постановления Пленума ВС РФ можно узнать, что же является мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ). По словам судьи Верховного Суда Татьяны Хомицкой, в результате долгих обсуждений сошлись на том, что это «вмеша-

тельство в функционирование средств хранения, обработки и передачи информации». Данное постановление четко разделяет понятия «мошенничества в сфере компьютерной информации» и «кражи путем ввода информации». Например, хищение денежных средств путем использования «мобильного банка» другого человека следует считать кражей, а не мошенничеством [1, с. 32]. Также необходимо оценивать и мошенничество путем создания поддельных интернет – магазинов. Данное деяние будет квалифицироваться по ст. 159 УК РФ, а не по ст. 159.6 УК РФ.

Новое постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» раскрывает смысл статьи 159.6 УК РФ, а именно: «вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него».

Кроме того, в Пленуме указано, что совершенное посредством неправомерного доступа к компьютерной информации мошенничество, а также распространение вредоносных компьютерных программ требует дополнительной квалификации по ст.ст. 272, 273, 274.1 УК РФ. При рассмотрении ст.ст. 272 УК РФ и 159.6 УК РФ можно заметить, что в первой используется фраза уничтожение компьютерной информации, тогда как во второй – удаление компьютерной информации. Нужно отметить, что данные понятия обозначают разные вещи. Уничтожением является прекращение существования чего-либо, истребление, тогда как удаление лишь отдаление доступа к информации. Отсюда следует, что уничтожение не квалифицируется ст. 159 УК РФ. В случае хищения путем уничтожения информации нужно дополнительно обратиться к ст.ст. 272–273 УК РФ.

В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием [3, с. 131].

В случае, когда хищение чужого имущества осуществляется с помощью создания заведомо ложных сведений в сети «Интернет» или других различных телекоммуникационных сетях, с помощью, например, создания ложных сайтов, то такое мошенничество квалифицируется по ст. 159 УК РФ.

Таким образом, новое постановление Пленума Верховного Суда внесло определенные разъяснения по квалификации мошенничества в сфере компьютерной информации. Однако это не последнее разъяснение Пленума по данному вопросу. И, прежде чем законодатель обобщит всю имеющуюся практику и придет к единому мнению по квалификации данного преступления, пройдет немало времени.

Библиографический список

1. Русскевич Е. А. Разъяснения Пленума ВС РФ о квалификации мошенничества в сфере компьютерной информации // Уголовный процесс. – 2018. – № 2. – С. 33.

2. Гончар В. В., Мешков М. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования // Мировой судья. – 2015. – № 4. – С. 14–18.

3. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

Н. В. Макеева[1], *А. В. Макеев* [2]

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ РЕШЕНИИ ВОПРОСА О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО НЕЗАКОННОМУ СБЫТУ НАРКОТИЧЕСКИХ СРЕДСТВ БЕСКОНТАКТНЫМ СПОСОБОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Федеральным законом от 01 марта 2012 г. № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в ст. 228.1 Уголовного кодекса Российской Федерации были внесены изменения, согласно которым была установлена ответственность за незаконный сбыт наркотических средств, психотропных веществ или их аналогов, совершенных с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). Такой способ сбыта на практике и в юридической литературе принято называть «бесконтактным способом сбыта наркотических средств». Это под собой подразумевает сбыт наркотиков новым способом, когда сбытчик и незаконный приобретатель не встречаются лично, а договариваются о приобретении наркотических средств, оплачивают их получение, получают сведения о местонахождении тайника с использованием мобильной связи или сети «Интернет». Появляющиеся новые способы сбыта, заставляют сотрудников органов внутренних дел менять способы фиксации сбыта в том числе, с использованием материалов оперативно-разыскной деятельности.

Согласно действующему законодательству [1] и результаты ОРД могут:

– служить поводом и основанием для возбуждения уголовного дела;

– быть использованными для подготовки и осуществления следственных и судебных действий;

– использоваться в доказывании по уголовным делам.

Как показывает практика, самым распространенным поводом для возбуждения уголовных дел, связанных с незаконным оборотом нар-

---

[1] Доцент кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук, доцент. © Макеева Н. В., 2018.

[2] Старший преподаватель кафедры организации деятельности ОВД ЦКШУ Академии управления МВД России кандидат юридических наук. © Макеев А. В., 2018.

котических средств, психотропных веществ, является рапорт об обнаружении признаков преступления. Основанием для возбуждения уголовного дела в рамках указанного повода служат материалы, полученные в ходе осуществления оперативно-разыскных мероприятий.

Чаще всего при поступлении информации о факте совершения противоправных действий, связанных с незаконным оборотом наркотических средств или психотропных веществ, осуществляются такие оперативно-разыскные мероприятия, как: проверочная закупка; наблюдение; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров.

Особенностью бесконтактного способа сбыта является то, что сбыт чаще всего осуществляется организованной группой, в которой все роли четко распределены. В структуру группы входят: организатор, оператор, закладчик, вербовщик, кладовщик, системный администратор, экспедитор [2, с. 78–81, с. 215–217, с. 68–73]. Вступая между собой в преступный сговор эти лица действуют с использованием удаленного сервера, электронных и информационно-телекоммуникационных сетей, размещают информацию о виде, весе, цене предлагаемого наркотика, а также способах связи и оплате на сайтах в сети «Интернет». При этом после поступления денежных средств на электронные платежные системы (QIWI-банк; Яндекс.Деньги; WebMoney) осуществляют передачу наркотических средств через систему тайников, место расположение которых сообщают после оплаты с помощью средств мобильной связи. Такой способ сбыта характеризуется тем, что нижестоящие участники не знают вышестоящих. Это осложняет процесс их выявления и доказывания незаконной деятельности организованной группой.

В связи с этим органами внутренних дел отрабатываются алгоритмы деятельности, в том числе связанные с фиксацией факта сбыта бесконтактным способом на этапе возбуждения уголовного дела. Особенностью деятельности на этом этапе являются: длительное документирование факта преступной деятельности, привлечение значительного числа технических средств и специалистов оперативно-технических подразделений, координация действий с высококвалифицированными следователями.

Следует обратить внимание, что в п.13 постановления Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 «О судебной практике

по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» были внесены изменения, согласно которым теперь может квалифицироваться как незаконный сбыт наркотических средств не только зафиксированный факт возмездной либо безвозмездной передачи наркотиков (с поличным, как этого ранее требовало законодательство), но вообще любая деятельность, направленная на их возмездную либо безвозмездную реализацию другому лицу. При этом передача сбытчиком наркотического средства может осуществляться любым способом, в том числе и путем сообщения приобретателю о месте его хранения, проведения закладки в обусловленном месте.

Особое следует заметить, что в п. 13.1 Пленума разъяснено, что незаконный сбыт следует считать оконченным преступлением с момента выполнения лицом всех необходимых действий по передаче приобретателю указанных средств, веществ, растений независимо от их фактического получения приобретателем, в том числе когда данные действия осуществляются в ходе проверочной закупки или иного оперативно-разыскного мероприятия.

Таким образом, в рамках осуществления оперативно-разыскных мероприятий не требуется обязательного фиксирования факта непосредственной передачи (из рук в руки) наркотических средств для вменения лицу сбыта наркотических средств.

Тем не менее, для фиксирования незаконного сбыта наркотических средств требуется проведение одного или нескольких ОРМ. В зависимости от поступившей оперативной информации это может быть:

– обследование помещений, зданий, сооружений, участков местности, когда поступает информация о точном месте нахождения закладки с наркотиками;

– наблюдение за лицом, производящим закладку наркотиков;

– проверочная закупка, которая остается наиболее характерным ОРМ, осуществляемым, в том числе, при фиксации бесконтактного способа сбыта. При этом обмен информацией о наркотическом средстве, месте, времени его закладки и оплата осуществляются с использованием сети «Интернет». Особенностью является то, что при бесконтактном способе сбыта непосредственного контакта во время проверочной закупки между сбытчиком и покупателем не происходит.

Основными условиями признания законности проведенных оперативно-разыскных мероприятий и дальнейшего использование его результатов при принятии решения о возбуждении уголовного дела и в

дальнейшем в доказывании по уголовному делу [3, с. 22–27] является наличие объективной информации о фактах незаконного сбыта наркотических средств и психотропных веществ конкретным лицом или группой лиц, а также:

1) их осуществление для решения задач, определенных ст. 2 ФЗ «Об ОРД», при наличии оснований и с соблюдением условий, предусмотренных ст.ст. 7 и 8 указанного Федерального закона (так, условием законности производства проверочной закупки наркотических средств является проведение ее на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-разыскную деятельность);

2) результаты оперативно-разыскного мероприятия могут быть положены в основу приговора, если они:

– получены в соответствии с требованиями закона;

– свидетельствуют о наличии у лиц умысла на незаконный оборот наркотических средств и психотропных веществ, сформировавшегося независимо от деятельности сотрудников оперативных подразделений (п.14 постановления Пленума Верховного Суда РФ от 15 июня 2006 г. № 14).

Вышеуказанное имеет особое значение для ОРД, поскольку в соответствии с действующим законодательством недопустимы провокационные действия со стороны оперативного работника, направленные на побуждение лица к совершению преступления.

В частности, соблюдение законности в рамках проведения и фиксации результатов проверочной закупки позволит в дальнейшем использовать материалы ОРМ при решении вопроса о возбуждении уголовного дела.

Получив материалы ОРМ, следователь осуществляет проверку результатов оперативно-разыскной деятельности на предмет их соответствия требованиям закона, после чего принимает меры к приданию им доказательственного значения. Результаты ОРМ в дальнейшем в случае их законного происхождения служат поводом и основанием для возбуждения уголовного дела и используются в доказывании по уголовным делам. Если в материалах проверки есть сведения, указывающие на использование информационно-телекоммуникационных сетей, то следователь должен квалифицировать действия по п. «б» ч. 2 ст. 228.1 УК РФ. Несмотря на существующие явные проблемы, связанные со сложным процессом выявления и фиксирования преступлений, совершенных бесконтактным способом, на сегодняшний день та-

кого рода преступления успешно расследуются органами предварительного следствия и в судах по ним выносятся обвинительные приговоры [4, с. 27].

Библиографический список

1. Приказ МВД России от 27 марта 2013 г. № 776/703/509/507/1820/42/ 535/ 398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // Российская газета. – 2013. – № 282. – 13 дек.

2. Помелов А. А. Некоторые вопросы документирования сбыта наркотических средств с использованием сети «Интернет». XXI Международная научно-практическая конференция «Деятельность правоохранительных органов в современных условиях». – Иркутск, 2016.

3. Пушкарев В. В. Теоретические основы разыскной деятельности следователя по уголовным делам о серийных преступлениях // Вестник Московского университета МВД России. – 2015. – № 10.

4. Радченок Т. В. Особенности квалификации хищения наркотических средств или психотропных веществ, совершенного с применением насилия // Эпоха науки. – 2017. – № 11.

5. Титовец И. В. Действие норм о недопустимых доказательствах при проверки заявлений и сообщений о преступлении // В книге: социально-экономические и правовые меры борьбы с правонарушениями тезисы научно-практической конференции. 2015.

6. Орлова А. А., Гончар В. В., Батюк В. И., Мешков М. В. и др. Предварительное следствие в органах внутренних дел : учебное пособие / под ред. М. В. Мешкова. – М. : Щит-М, 2007.

С. В. Ермаков[1]

УГОЛОВНОЕ СУДОПРОИЗВОДСТВО В СВЕТЕ РЕАЛИЗАЦИИ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА РОССИЙСКОЙ ФЕДЕРАЦИИ»

В настоящее время политика государства направлена на максимально возможное использование цифровых технологий во всех сферах социально-экономических отношений. Так, распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р утверждена Программа «Цифровая экономика Российской Федерации» [1]. Органами государственной власти приняты акты, обеспечивающие развитие цифровой экономики, такие как: Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 г.; Прогноз социально-экономического развития/научно-технологического развития до 2030 года; Стратегия научно-технологического развития; Стратегия развития отрасли информационных технологий РФ на 2014–2020 годы и на перспективу до 2025 года; Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы; Государственная программа «Информационное общество»; План мероприятий («дорожная карта»); Развитие отрасли информационных технологий и другие [2].

С использованием цифровой экономики предполагается осуществить переход к новому технологическому укладу. Современные тенденции развития информационного общества подталкивают к мысли о том, что и уголовно-процессуальная деятельность также должна развиваться в данном направлении.

Российское уголовное судопроизводство является исторически сложившимся механизмом процессуального познания обстоятельств совершенных преступлений, установления лиц, их совершивших, и привлечения виновных к уголовной ответственности. Существующие методы сбора, хранения, передачи информации в рамках уголовного судопроизводства чрезвычайно формализованы, достаточно консервативны, что не позволяет развиваться уголовно-процессуальной деятельности «в ногу со временем». Внутриведомственное и межведомственное взаимодействие участников уголовного судопроизводства также закрепощено бумажно-бюрократической формой. Бумажная работа занимает значительное время в уголовно-процессуальной дея-

---

[1] Заместитель начальника кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя кандидат юридических наук. © Ермаков С. В., 2018.

тельности. В таких условиях трудозатраты на осуществление уголовного судопроизводства являются весьма значительными. Значительные нагрузки на сотрудников органов предварительного расследования обусловливают отток кадров, а увеличение количества должностей дознавателей, следователей, прокуроров и судей в условиях дефицита бюджета является невозможным.

В связи с этим необходимо искать способы решения задачи по сокращению времени, затрачиваемому дознавателями, следователями, прокурорами, судьями на техническую работу. Внедрение новых цифровых технологий может способствовать решению данной задачи.

Нельзя отрицать тот факт, что уголовно-процессуальное законодательство пытается не отставать от современных цифровых реалий. Так, например, введены нормы, затрагивающие вопросы изъятия и признания вещественными доказательствами электронных носителей цифровой информации (ст.ст. 81.1, 182, 183 УПК РФ). Федеральным законом от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» УПК РФ дополнен ст. 474.1, определяющей порядок использования электронных документов в уголовном судопроизводстве. В частности, допускается подача в суд ходатайств, заявлений, жалоб, представлений в форме электронного документа, подписанного электронной подписью, а также судебное решение может быть в виде электронного документа, подписанного усиленной квалифицированной электронной подписью.

Однако информатизация уголовного судопроизводства, особенно досудебной его части, на сегодняшний момент явно отстает от стоящих перед государством задач по развитию информационного общества. При изменении уголовно-процессуального законодательства необходимо учитывать стремительность развития новых цифровых технологий. Уголовно-процессуальное законодательство объективно выступает в роли «догоняющего» и развивается лишь вслед за изменениями общественных отношений.

Много доводов можно привести в пользу сохранения существующей «бумажно-бюрократической» системы уголовного судопроизводства. Это, прежде всего: необходимость сохранения тайны следствия; низкий уровень компьютерной грамотности как следователей, дознавателей, прокуроров, защитников, так и граждан, вовлеченных в данную сферу; недостаточные технические возможности органов предварительного расследования, прокуратуры, судов для перехода в цифровую

среду (наличие компьютерной техники, серверов для хранения информации, систем информационной безопасности); отсутствие электронных цифровых подписей у большинства граждан и должностных лиц.

В настоящий момент развития информационного общества можно утверждать, что введение информационных технологий в процессы уголовного судопроизводства будет возможно лишь после реализации программы цифровой экономики других сферах общественной жизни [4, 5]. Необходимо формирование соответствующей информационной среды. В частности, наличие электронных паспортов у граждан, использование электронной подписи всеми гражданами и должностными лицами, биометрическая идентификация личности и прочее.

В ряде стран такие условия уже формируются. Стоит рассмотреть положительный опыт Эстонии. Там, начиная с 2002 г, начали выдавать электронные паспорта, которые способны удостоверять личность и в реальной жизни, и в цифровом пространстве. Встроенный в паспорт чип содержит информацию о гражданине и цифровую подпись. Эстонская система электронных паспортов признана одной из лучших в ЕС [3].

Биометрическая идентификация личности имеет большой потенциал в сфере борьбы с преступностью, в том числе для деятельности «электронной» полиции. Целесообразно введение обязательной биометрической идентификации граждан Российской Федерации в случаях получения, замены паспорта, а также иностранных граждан при въезде на территорию Российской Федерации.

Таким образом, систему идентификации физических лиц необходимо связывать прежде всего с функцией подписания электронных документов, что обеспечит переход на электронный уровень общения должностных лиц, в том числе правоохранительных органов с гражданами. Необходимо обеспечить возможность всех лиц представлять электронные документы должностным лицам правоохранительных органов. При этом подписание документа электронной подписью минимизирует случаи обращения граждан с ложными заявлениями и обращениями, в том числе о преступлениях. Данные технологии уже применяются в правовой сфере. Так, приказом Судебного департамента при Верховном Суде Российской Федерации от 28 декабря 2016 г. № 252 утвержден Порядок подачи документов в электронном виде, в том числе в форме электронного документа. Приказом Судебного департамента при Верховном Суде Российской Федерации от 11 сентября 2017 г. № 168 «Об утверждении Порядка подачи мировым судьям

документов в электронном виде, в том числе в форме электронного документа».

Уже сейчас объективно используется, но при этом является законодательно неурегулированной процедура передачи различных материалов, документов по электронной почте, на электронных носителях между участниками уголовного судопроизводства. Дознаватели, следователи, прокуроры, судьи обязаны уведомлять участников уголовного судопроизводства о принятых решениях, предоставлять копии процессуальных документов, рассматривать жалобы.

В будущем возможно создание личных кабинетов для участников уголовного судопроизводства по аналогии с порталом государственных услуг. Например, заявитель через личный кабинет может подавать заявление, уведомляется о принятии решения о возбуждении уголовного дела или отказе в возбуждении уголовного дела. Для потерпевшего личный кабинет предоставит возможность знакомиться с постановлением о назначении экспертизы, иными материалами уголовного дела в части, его касающейся, обжаловать действия должностных лиц. Обвиняемый сможет знакомиться с обвинительным заключением, обвинительным актом (постановлением), а подсудимый – с приговором или иным решением суда.

Внедрение электронной формы документооборота целесообразно и в сфере оказания международной правовой помощи по уголовным делам. В настоящее время запросы об оказании правовой помощи по уголовным делам исполняются крайне долго, в том числе в связи с бумажной формой передаваемых документов.

В части развития информатизации уголовного судопроизводства можно указать на потенциальные возможности использования современных и перспективных технологий цифровой экономики.

1. Технологии виртуальной и дополненной реальностей. Их можно использовать при осмотре места происшествия. Так, в США применяются технологии, которые позволят во всех подробностях переносить внешний вид различных мест преступления в виртуальный мир. Судьи и присяжные заседатели при рассмотрении дела могут осматривать места происшествий при помощи очков виртуальной реальности.

2. Большие данные (синонимы – супермассивы данных, BIG DATA). Супермассивы данных – огромные объемы внутренних и внешних данных различной структуры (таблицы, текст, изображение, голос, видео и др.). Такие данные являются информацией, представленной в цифро-

вом виде. Они могут накапливаться и правоохранительными органами. Большие данные – это, прежде всего, новые возможности для осуществления аналитики, выявление скрытых зависимостей и поиск новых вопросов и ответов на основе анализа всего объема разнородных данных. Примечательно, что данные сами определяют новые вопросы и формулируют ответы на них. В расследовании преступлений использование «больших данных» – весьма перспективное направление, т. к. с их использованием появится возможность более объективно прогнозировать совершение преступлений, выдвигать версии, планировать расследование преступлений, организовывать розыск скрывшихся от следствия и суда подозреваемых и обвиняемых.

3. Искусственный интеллект. Технологии искусственного интеллекта могут быть реализованы в автоматизированных онлайн-помощниках должностных лиц уголовного судопроизводства, в чат-ботах на веб-сайтах правоохранительных органов. Искусственный интеллект можно использовать для анализа и собирания информации о человеке, оценке его психоэмоционального состояния. Так, в ОАЭ уже существует робот-полицейский, который умеет говорить на шести языках, ориентируется на местности, на расстоянии полутора метров в состоянии распознавать жесты руками, а также настроение людей, считывая выражение лица человека.

Подводя итог, отметим, что в ближайшее время информационные технологии не смогут полностью заменить умственную работу дознавателя, следователя, прокурора, судьи, однако возможности, которые они предоставляют, могут быть эффективно внедрены и использованы в уголовно-процессуальной деятельности.

Библиографический список

1. Собр. законодательства Рос. Федерации. – 2017. – № 32, ст. 5138.
2. Официальный интернет-портал правовой информации» (www.pravo. gov.ru).
3. https://kaktus.media/doc/325581_biometriia._ne_tak_strashen_ chip_kak_ ego_maluut._opyt_estonii.html (дата обращения 31.01.2018).
4. Захаров Д. Н., Щерба В. В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2 (т. 2).
5. Захаров Д. Н., Иванов В. Ю. Безопасность в сфере оборота виртуальной валюты // Вопросы кибербезопасности. – 2017. – № 2 (20). – С. 30–38.

Раздел 6. ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

А. В. Костюк[1], *А. И. Примакин*[2]

К ВОПРОСУ ОБ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА

Проблема информационной безопасности различных государственных, производственных и общественных объектов причисляется к области государственной политики и уже в течение длительного времени остается злободневной как в теоретическом, так и в прикладном плане [1]. Изменение упоров и приоритетов в трактовке проблемы информационной безопасности и перенос их на нужды индивидуума с интересов государства поставили науку и практику перед потребностью исследования вновь появившейся проблемы, а именно: разработку вопросов обеспечения информационно-психологической безопасности личности [2].

Информационно-психологическая безопасность (ИПБ) личности, как составная часть информационной безопасности, связана в основном с отсутствием (недостатком) необходимой информации; нарушением прав личности в сфере доступа к информации; с воздействием информации сомнительного характера и другими информационными воздействиями на психику личности, что бесспорно ухудшает интеллектуальное, духовно-нравственное состояние человека и угрожает его здоровью.

Анализ научной литературы позволяет выделить некоторые из видов недоброкачественной («вредоносной») информации, которая способна привести к серьезным отклонениям в психике человека. К видам такой информации следует отнести:

– информацию, порождающую религиозную, расовую или национальную ненависть;

– информацию, порождающую воинственные настроения;

---

[1] Профессор кафедры информатики и математики Санкт-Петербургского военного института войск национальной гвардии Российской Федерации кандидат технических наук, доцент. © Костюк А. В., 2018.

[2] Начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России доктор технических наук, профессор. © Примакин А. И., 2018.

– информацию, содержащую элементы ненависти, вражды и превосходства;

– информацию, содержащую посягательства на честь, доброе имя и репутацию личности;

– информацию, содержащую элементы неосознаваемого деструктивного воздействия на психику людей.

Одним из основных неблагоприятных явлений, которое привело к возникновению угроз ИПБ личности, является лавинообразное увеличение объемов всех видов информации. Такое явление в литературе именуется как «информационный взрыв». Лавинообразный рост информации неизбежно ведет к тому, что человек не в состоянии воспринять, осмыслить, систематизировать даже те источники информации, которые нужны ему в профессиональной деятельности. Следствием этого явилось перенасыщение информационной среды.

«Информационный взрыв» неизбежно ведет к информационному стрессу. Данная болезнь приводит к снижению способности отбирать, оценивать и сохранять информацию. На уровне принятия решения информационные перегрузки могут вызывать стресс решений (неспособность личности принимать любые решения). Иным отрицательным информационным фактором, который оказывает влияние на психику человека и даже на его душевно-нравственные устои, предстает существенное «загрязнение» информационной среды.

В научной литературе ИПБ личности трактуется как уровень защищенности ее психики от воздействия разнообразных информационных факторов, мешающих или затрудняющих создание и функционирование соответствующей информационно-ориентировочной основы жизнедеятельности человека в обществе, а также адекватной системы его персональных отношений к окружающему миру и самому себе [2].

В общем виде ИПБ следует трактовать как степень защищенности индивидуальной, групповой и общественной психологии от деструктивного влияния негативных информационных факторов на сознание.

Объективная неосуществимость уберечь личность от всевозможных отрицательных информационно-психологических воздействий сдвигает «центр тяжести» проблемного вопроса обеспечения ИПБ личности на развитие ее «иммунитета» к подобным информационным влияниям, что смещает данную проблему в психолого-педагогическую плоскость.

Обучение личности в области ИПБ необходимо направить на формирование знаний, умений и навыков, которые обеспечили бы безо-

пасность человека и включили бы обучение человека знанию возможных опасностей, внешних и внутренних угроз, способов защиты, оказывали бы содействие в понимании потребности и возможности защиты, а также способствовали бы овладению необходимыми умениями. В границах данного подхода можно также рекомендовать формы психологической подготовки специального назначения, в частности тренинги, которые обеспечивали бы приобретение опыта противодействия информационно-психологическому воздействию [3].

Другой подход базируется на осмыслении ИПБ как состояние жизнедеятельности человека, при котором может уменьшаться с течением времени вероятность реализации личностью жизненных целей и затрудняться его развитие. С точки зрения такого подхода одним из ключевых условий обеспечения ИПБ личности является наличие у человека устойчивой системы жизненных ценностей и последующая их реализация.

Задачи информационного и психологического образования в сфере ИПБ человека целесообразно объединить в три блока [3]:

1) содействие подрастающей личности в самопознании, формирование умений самоконтроля, саморегуляции, самоорганизации;

2) содействие в постижении своей системы ценностей, поддержка процесса выработки персонального пути к преодолению актуальных противоречий, выбора;

3) помощь в формировании взглядов, которые содействовали бы становлению положительного эмоционально-ценностного восприятия себя, других людей, саморазвития и своей безопасности.

Узловые источники угроз ИПБ по отношению к личности рассматриваются в основном как внешние и внутренние. К внешним угрозам следует отнести соответствующие воздействия разнообразных организаций и людей, средств массовой информации и пр. С этих позиций формирование информационно-психологической безопасности требует создание надлежащей системы противостояния по отношению к внешним угрозам. Такая система должна состоять из нормативно-правовой, организационной и технологической составляющих [4].

Большее количество внешних угроз личности содержит информационная сфера, в частности:

– недостаточно полная информация или отсутствие нужных сведений;

– незаконное ограничение доступа к открытым информационным ресурсам;

– двойственность информации и др.

Таким образом, можно сделать вывод о том, что обеспечение информационно-психологической безопасности личности является развитие ее ценностно-смысловой сферы и критического мышления, которое всецело и целиком основывается на мировоззрении человека. Кроме того, информационная культура личности может стать одним из краеугольных камней в формировании информационной безопасности личности, т. к. она является подсистемой личности, которая обеспечивает требуемый характер процессов ее жизнедеятельности.

Библиографический список

1. Костюк А. В., Бобонец С. А., Флегонтов А. В. Информационные системы и технологии. Информационные технологии. Базовый курс : учебник. Ч. 2.– СПб. : Изд. РГПУ имени А.И. Герцена, 2014. – 308 с.

2. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. URL: htpp// bookap.by.ru/psywar/grachev.

3. Бобонец С. А., Костюк А. В. Обеспечение безопасности электронного обучения // Направления и перспективы развития образования в военных институтах внутренних войск МВД России : материалы VII Международной научно-практической конференции: в 2 ч. – Новосибирск : НВИ войск национальной гвардии, 2017. – С. 102–104.

4. Лызь Н. А., Непомнящий А. В. Безопасность как характеристика личности // Известия ТРТУ (Таганрог). – 2002. – № 5 (28). С. 168–173.

А. Н. Сударик[1]*, С. В. Здорова*[2]

ПСИХОЛОГИЧЕСКИЕ ПРЕДПОСЫЛКИ СОЦИАЛЬНОЙ НЕЗАЩИЩЕННОСТИ ГРАЖДАН В КОММУНИКАТИВНОЙ СФЕРЕ ПРИ ПРИМЕНЕНИИ ВЫСОКИХ ТЕХНОЛОГИЙ

С каждым годом технические системы защиты все больше и больше совершенствуются за счет постоянного развития современных информационных технологий, учета множества потребностей и различных рисков. Грамотно отстроенные технические системы защиты длительное время могут исправно выполнять свои основные функции и задачи. Что нельзя сказать о человеке. Люди так и будут оставаться людьми, со своими слабостями, предрассудками, стереотипами, являясь самым слабым звеном в цепочке безопасности.

Основная мысль, сформулированная международным экспертом по безопасности Брюсом Шнайером, о том, что «безопасность – это непрерывный процесс, а не результат», и избавляет нас от иллюзии абсолютной защищенности как отдельно взятого человека, так и организаций в целом.

При намеренном воздействии (атаке) на человеческий фактор, при котором нарушается психологическая безопасность личности, самые совершенные и дорогостоящие системы защиты становятся ненужными, неэффективными, попросту игрушками. В современном мире такое воздействие принято называть социальной инженерией.

В связи с этим обеспечение надежности человеческого фактора в цепочке безопасности можно рассматривать в контексте изменения человеческой психологии, наделения ее необходимыми качествами, которые смогут противостоять деструктивным технологиям социальной инженерии.

Проблеме обеспечения надежности сотрудников ОВД посвящено ряд работ [1]. Однако, данную проблему предлагается решать в контексте создания модели личностно-профессиональной надежности и использования ее для решения задач профессионально-психологического отбора.

---

[1] Заместитель начальника кафедры психологии УНК психологии служебной деятельности МосУ МВД России имени В.Я. Кикотя кандидат психологических наук. © Сударик А. Н., 2018.

[2] Старший инспектор группы по работе с переменным составом факультета подготовки специалистов в области информационной безопасности МосУ МВД России имени В.Я. Кикотя. © Здорова С. В., 2018.

В современной научной литературе развиваются различные подходы к пониманию психологической безопасности личности, группы и общества. Психологическую безопасность рассматривают с позиции развития личностно-психологических особенностей человека, которые выступают субъективными условиями для формирования безопасности [2]. Феномен психологической безопасности человека изучается как уровень или характеристика его качества жизни [3]. Психологическая безопасность личности трактуется как предметно-преображающая активность субъекта в парадигме самоутверждения и самореализации [4]. Наряду с рассмотрением в зарубежной литературе социально-философских проблем общества риска в отечественной науке разрабатываются идеи связей факторов риска и психологической безопасности личности и общества [5].

Значительный вклад в развитие и становление психологии безопасности внесли исследования, которые рассматривают компоненты психологической безопасности с точки зрения субъектов взаимодействия [6].

В современной психологической науке понятие безопасности используется в различных аспектах изучения жизнедеятельности человека. Основные направления, по которым развиваются исследования психологической безопасности в отечественной науке, кратко представлены О. Ю. Зотовой [7]. Исследования феномена безопасности в психологии в той или иной степени всегда сопряжены с методологическими и теоретическими затруднениями. Безопасность, с одной стороны, является фундаментальным понятием, с другой – крайне широким и многогранным понятием.

Кроме этого безопасность является и инструментом, и эталоном, в соответствии с которым может происходить оценка действий, событий и ситуаций.

Под психологической безопасностью любой социальной среды понимается состояние, свободное от проявлений психологического насилия во взаимодействии, способствующее удовлетворению потребностей в личностно-доверительном общении, создающее референтную значимость среды и обеспечивающее психическое здоровье включенных в нее участников [8].

Именно общение участников любого социального процесса, специально организованные психолого-педагогические условия и возможности реализации этого общения в социальной среде «порождают» психологическую безопасность личности. Общение порождает, созда-

ет и референтную значимость среды, и психологическую защищенность ее участников, и удовлетворенность отдельными компонентами самого взаимодействия.

Таким образом, сфера общения является той социальной средой, в которой возможно осуществление намеренного воздействия на личность в целях нарушения ее психологической безопасности, которое может проявляться в различных формах обмана, завлечения в сомнительные сделки и другие непродуктивные мероприятия в ущерб личным интересам граждан.

В психологической структуре личности имеются психологические конструкты, опираясь на которые возможно анализировать предрасположенность человека к доверительному общению и способность его контролировать ситуации общения.

Методика диагностики коммуникативной установки В. В. Бойко позволяет определить коммуникативные свойства личности испытуемых, препятствующие осуществлению ими эффективных коммуникаций. Методика содержит 24 вопроса и пять шкал: завуалированная жестокость, открытая жестокость, обоснованный негативизм, брюзжание и негативный опыт общения. Одноименные показатели негативной коммуникативной установки (НКУ) измеряются в баллах и определяются по ключу. При этом если испытуемый получает общий балл выше общего среднего – 33 балла, это свидетельствует о наличии выраженной общей негативной коммуникативной установке (НКУ «-»), которая, по всей вероятности, неблагоприятно сказывается на самочувствии партнеров. В противном случае (НКУ «+») негативная коммуникативная установка не проявляется, не оказывает существенного влияния на окружающих. Аналогично выраженность НКУ по каждой шкале определяется относительно критического значения, определяемого на уровне 33% от максимального балла, который может набрать испытуемый по каждой шкале.

Используя направленность показателей коммуникативной установки, а также изучая индивидуально-психологические характеристики граждан такие, как: A – «замкнутость–общительность», E – «подчиненность – доминантность», G – «подверженность чувствам – высокая нормативность поведения», H – «робость-смелость», L – «доверчивость – подозрительность», O – «уверенность в себе – тревожность», Q_3 – «низкий самоконтроль – высокий самоконтроль» Q_2 – «конформизм – нонконформизм», спонтанность – сензитивность, агрессивность – тревожность, ригидность – лабильность, лидерство – зависи-

мость, возможно выделить детерминирующие факторы, влияющие на коммуникативные свойства различных категорий граждан в условиях использования высоких технологий для осуществления общения.

Гуманистическая психология утверждает, что для того чтобы постичь человеческую природу, понять ее возможности, надо создать особого рода условия, благоприятствующие выражению позитивных потребностей (Дж. Бюджентал, А. Маслоу, К. Роджерс, Р. Снайдер и др.).

Такой методологический подход к процессу совершенствования системы защищенности граждан от технологий социальной инженерии требует построения контртехнологий формирования психологической защищенности граждан с учетом их индивидуально-психологических особенностей.

В рамках обозначенного подхода для обеспечения эффективных коммуникаций по результатам эмпирического исследования компонентов коммуникативного потенциала, относящихся к коммуникативным свойствам и способностям личности, и применения в ходе обработки данных однофакторного дисперсионного анализа выявлены определенные влияния на указанные компоненты психологических факторов, измеряемых методиками Р. Б. Кетелла и Л. Н. Собчик [9].

Для обеспечения психологической безопасности и повышения защищенности личности в сфере высоких технологий целесообразно проверить пилотные исследования по предложенной схеме и разработать рекомендации по развитию у граждан эффективных защитных механизмов от негативного воздействия приемов и техник социальной инженерии.

Библиографический список

1. Кравченко А. В., Еременко Т. Е. Моделирование личностно-профессиональной надежности участковых уполномоченных полиции // Юристъ. – Правоведъ. – 2017. – № 2 (81). – С. 116–119.

2. Донцов А. И., Перелыгина Е. Б. Проблемы безопасности коммуникативных стратегий // Вестник Московского университета. Серия 14. Психология. – 2011. – № 4. – С. 24.

3. Краснянская Т. М., Тылец В. Г. Темпоральные аспекты психологической безопасности // Изв. Сарат. ун-та. Серия: Философия. Психология. Педагогика. – 2015. – Т. 15. Вып. 3. – С. 70–75.

4. Зинченко Ю. П., Бусыгина И. С. Психологическое здоровье и профессиональная самореализация руководителя // Национальный психологический журнал. – 2013. – № 1 (9). – С. 89–95.

5. Корнилова Т. В. Индивидуальные категории субъективного риска // Вопросы психологии. – 1999. – № 6. – С. 128–139.

6. Баева И. А. Общепсихологические категории в практике исследования психологической безопасности образовательной среды // Известия российского государственного педагогического университета имени А. И. Герцена. – 2010. – № 128. – С. 27–39.

7. Зотова О. Ю. Современные отечественные концепции психологии безопасности // Человеческий капитал. – 2016. – № 4 (88). – С. 133–134.

8. Баева И. А. Психологическая безопасность в образовании: монография. – СПб. : СОЮЗ, 2002. – 271с.

9. Сударик А. Н. Детерминация факторов развития коммуникативной компетентности курсантов-психологов в образовательной среде вуза МВД // В сборнике: Молодые исследователи образования. Тезисы конференции. – 2017. Том. II. – С. 170– 172.

10. Сударик А. Н. Коммуникативная компетентность курсантов-психологов: исследование детерминирующих факторов развития в образовательной среде вуза МВД // В сборнике: Современные подходы в оказании экстренной психологической помощи : материалы V Всероссийской научно-практической конференции / под ред. А. В. Кокурина, В. И. Екимовой, Е. А. Орловой. – М. : РУСАЙНС, 2017. – С. 293–298.

Л. Б. Ткаченко[1]

ИСПОЛЬЗОВАНИЕ ПРАВОНАРУШИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАСПРОСТРАНЯЕМЫХ ПОДРОСТКАМИ В СЕТИ «ИНТЕРНЕТ»

Мир, в котором живем мы и наши дети, разительно отличается от того, каким он был каких-нибудь пару десятков лет назад. Информационные технологии позволяют нам сиюминутный доступ к любой информации, удобно, это открывает массу возможностей. Отметим, что значительное число пользователей сети «Интернет» – дети и подростки.

Разумеется, непременной обратной стороной медали явился вал негативных моментов, к которым отнесем бесконтрольное распространение информации, противозаконные операции с электронными деньга-

[1] Старший преподаватель-методист кафедры предварительного расследования МосУ МВД России имени В.Я. Кикотя. © Ткаченко Л. Б., 2018.

ми, преступления, касающиеся персональных данных, хранящихся на жестких дисках пользователей, и априори неподлежащей распространению.

Современные социальные сети аккумулируют неимоверное количество персональных данных их участников. Причем безопасность таких сведений в нашем государстве регламентируется целым рядом законов. Далеко не все операторы, обрабатывающие такие данные, предпринимают шаги, направленные на обеспечение их безопасности. Иногда операторы намеренно уклоняются от выполнений требований закона сфере информационной безопасности. Одной из причин такого уклонения можно смело назвать нежелание расходовать средства на обеспечение безопасности и конфиденциальности указанной информации.

Среди опасностей, которые таит в себе существование в сети, отметим возможности манипулирования сознанием ребенка, подростка, неспособных противостоять тщательно продуманной и научно обоснованной манипуляции. Время, проведенное на просторах Интернет, способно привести к утрате чувства реальности окружающего мира.

Существует мнение о том, что значительное отличие Интернета от других современных технологий базируется на инициируемых ими же самими эффектах самоорганизации социокультурных систем. При этом не предусматривается возможность вероятности прогноза следствий этих эффектов в настоящем времени. Однако и это вполне оправдано исторически, система традиционных культурных ценностей и этических принципов не успевает за скоростью движущегося семимильными шагами НТП.

Болезненное пристрастие детей и подростков к высоким технологиям на наших глазах приводит к утрате смысла их существования вне сети. Само название «сеть» становится в данном конспекте именем нарицательным. Подкрепляется это, к сожалению, отсутствием или сведением к минимуму контроля со стороны взрослых, многим из которых такая «занятость» подрастающего поколения удобна или ошибочно выгодна. Не последнюю роль играет также неконкретность итогов развития отдельных видов высоких технологий, выступают серьезной опасностью для защиты подрастающего поколения и цивилизации в целом.

Как отмечает В. В. Гончар, проблема гипертрофированного пристрастия к Интернету в том, что «нынешнее» «цивилизованное», «глобализированное» общество не может дать четких критериев «хо-

рошего» и «плохого», «приемлемого» и «недопустимого». Четкие критерии отсутствуют и в области этики и морали, искусства и культуры. Интернет является частью современной культуры [1].

Социальные сети, сайты знакомств, форумы и мессенджеры сами по себе не несут угроз. Однако такая угроза вполне способна обнаружиться в методах их использования.

Что же можно отнести к аспектам опасности социальных сетей. Во-первых, такие ресурсы становятся основным способом общения, «извлекают» ребенка из реального мира и делают зависимым от себя.

Попавший в сложную жизненную ситуацию подросток, а также просто ребенок, желающий найти правильное решение или просто поддержку, способен впасть в истерику, не получив возможность пообщаться в социальной сети. Также значительным негативным показателей можно назвать то, что через подобные ресурсы к ребенку в доверие могут попасть разного рода злоумышленники и пытаться получить конфиденциальную информацию.

Большая часть мира использует глобальную сеть для тех или иных целей, но так или иначе абсолютное большинство пользователей вынуждены оставлять свои персональные данные, подписывая пользовательское соглашение. Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определенному физическому лицу (субъекту персональных данных) [2]. Определяя содержание пользовательского соглашения, законодатель приводит такое определение – заключение сторон договора, предусматривающее ряд условий между сторонами, среди которых, во-первых, предоставление пользователю сервисов в обмен на гарантии соблюдения режима пользования сервисами и согласие на получение рекламных объявлений (Федеральный закон № 152-ФЗ «О персональных данных»); во-вторых, санкции за несоблюдение условий договора.

В ФЗ № 152, как подчеркивалось ранее, к персональным данным относится информация, которая позволяет определить личность пользователя. Сюда относятся, прежде всего, фамилия, имя, отчество, дата и место рождения, адрес, телефон, семейное положение, паспортные данные, профессия и т. д.

Также законодательно установлено, что пароли к аккаунтам не являются персональными данными, поскольку, и это понятно, не содержат индивидуализированных данных о человеке. С согласия пользова-

теля данные могут становиться общедоступными, например, номер телефона или e-mail, которые передаются компании, но это обычно происходит при беглом изучении пользовательского соглашения. Тем не менее по требованию пользователя эти данные должны быть убраны из общего доступа согласно ст. 15 ФЗ № 152, п. 2 «Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных…» [2].

Известно, что, заключая пользовательское соглашение, многие пользователи не вчитываются внимательно в его смысл, объясняя это тем, что торопились, доверяли оператору или полагали, что договор составлен с участием юристов, используется не первый день и не должен содержать незаконных или негативных пунктов. Как мы понимаем, это рассуждение далеких от юридических тонкостей людей, большинство которых и не обязаны разбираться в этих тонкостях.

Получая доступ в безграничный мир информации, социальных и прочих сетей, пользователь находится, как правило, в собственной квартире или, используя свой мобильный телефон, другие гаджеты, использует пароли, что вызывает в нем ложное ощущение защищенности, при этом не понимает угрозы и, как следствие, недостаточно осторожен.

Получая информацию пользователи, так или иначе, оставляют информацию о себе. И это не просто фиксация IP-адреса, а персональные сведения на сайтах социальных сетей, пользователи одновременно становятся объектами внимания не только личных неприятелей, но и властных и коммерческих структур. Субъекты персональных данных передают данные каждый раз, когда авторизируются в сервисе и показывают свои предпочтения, переходя по страницам, которые их больше интересуют. Глобальный и постоянный анализ такой информации, по мнению автора, способен сделать человека абсолютно незащищенным.

Физически дотянуться до ребенка через Интернет невозможно. Но можно попытаться «выманить» его куда-то. Самым банальным является назначение свидания. Правонарушитель регистрируется как лицо противоположного пола, ставит себе привлекательную фотографию, приобретает доверие подростка, а потом предлагает встретиться в кафе поесть мороженое.

Не менее опасным способно стать манипулирование, исключающее визуальный контакт. Не для кого уже не секрет страшные подробности воздействия сайтов смерти на подростков.

В заключении следует отметить, что родители не редко из-за чрезмерного увлечения своей карьерой и личными делами, не могут уделять своим детям достаточного времени. Ребенок, не получающий от родителей должной заботы, чувствует себя одиноким, часто замыкается в себе и постепенно все сильней отчуждается от родителей и погружается в социальные сети, где находит себе единомышленников, а зачастую и людей, желающих воспользоваться его личной информацией с позиции обогащения. Кроме того, ребенок сознательно и неосознанно копирует поведение взрослых. И не важно, при этом, авторитетен ли для него взрослый.

Завоевать доверие ребенка можно, часто проявляя готовность общаться с ним. Ребенок должен чувствовать, что рядом с ним есть человек, которому он может поведать любые страхи и тревоги, рассказать о своих впечатлениях и наблюдениях, поделиться любой информацией. Общение и совместные мероприятия, в том числе спортивные и проходящие на открытом воздухе, очень сильно влияют на степень доверия между родителем и ребенком и служат весомой профилактикой в передаче личной информации правонарушителям.

Библиографический список

1. Гончар В. В. Влияние средств массовой информации на обучающихся : материалы международной научно-практической конференции «Формирование социокультурных компетенций в непрерывном образовательном процессе». – М. : МосУ МВД России, 2009. – С. 74.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «Консультант плюс». 2018.

О. Ю. Карлина[1]

НЕКОТОРЫЕ НЕГАТИВНЫЕ ФАКТОРЫ СЕТИ «ИНТЕРНЕТ», ФОРМИРУЮЩИЕ ЛИЧНОСТЬ ПОДРОСТКА-ПРАВОНАРУШИТЕЛЯ

Согласно данным статистики Генеральной прокуратуры Российской Федерации за 2017 г. суммарное количество киберпреступлений, зарегистрированных в Российской Федерации, составило 66 тыс., что, по словам Генерального прокурора Ю. Я. Чайки, в шесть раз больше по сравнению с аналогичным периодом 2011 г., а материальный ущерб от ИТ-преступлений для граждан и организаций составил свыше 18 млн долларов США. [1] Для сравнения, еще в 2003 г., всего по различным статьям, гл. 28 УК РФ было совершено 6 723 преступления.

Такая ситуация связана в первую очередь с развитием и созданием новых компьютерных технологий: увеличения мощности и функционала данных технологий в т. ч. для мобильных устройств, а также созданием новых систем хранения информации и управления. Во вторую очередь связано с тем, что использование современных технологий стало неизбежным атрибутом для большинства жителей нашей страны и в большинстве своем для всего остального мира, что приводит к повышению компьютерной грамотности и увеличению числа специалистов в компьютерной сфере.

Преступления в компьютерной сфере представляют серьезную угрозу ввиду высокой степени риска и значительного материального ущерба. Примечательно, что под «атаки» попадают как физические лица, так и крупные организации и банки, которые имеют убытки ежемесячно, хотя и обладают достаточными средствами и мощным аппаратом для защиты от таких преступных посягательств.

В мае 2017 г. в нескольких городах России задержаны два десятка киберпреступников, которые с помощью вредоносного ПО для мобильных устройств похитили более 50 млн руб.

Участники преступной группировки заразили более 1 млн смартфонов вредоносной программой Cron – троянцем для ОС Android, с помощью которого злоумышленники похищали денежные средства с банковских счетов. С помощью скрытых SMS-команд деньги переводились на заранее подготовленные счета [2].

---

[1] Московский педагогический государственный университет. © Карлина О. Ю., 2018.

Говоря об ИТ-преступлениях, можно смело утверждать, что незаконный доступ к компьютерной информации может повлечь за собой ряд негативных последствий: это и нарушение неприкосновенности интеллектуальной собственности, и разглашение сведений о частной жизни граждан, и имущественный ущерб в виде прямых убытков и недополученных доходов, и потеря репутации организации, и различные виды нарушений нормальной деятельности предприятия. Ввиду этого оправданно то, что преступления данного вида размещены в таком разделе, как «Преступления против общественной безопасности и общественного порядка».

Следует отметить, что уголовное законодательство разделяет преступления в сфере компьютерной безопасности на три основных вида:

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

– создание, использование и распространение вредоносных программ (ст. 273 УК РФ);

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) [3].

Следовательно, для совершения компьютерных преступлений злоумышленники используют:

– подбор паролей, ключей и другой идентификационной информации;

– подмену IP-адресов пакетов, передаваемых по Интернету или другой глобальной сети, так, что они выглядят поступившими изнутри сети, где каждый узел доверяет адресной информации другого узла;

– инициирование отказа в обслуживании – воздействие на сеть или отдельные ее части в целях нарушения порядка штатного функционирования;

– прослушивание и расшифровку трафика в целях сбора передаваемых паролей, ключей и другой идентификационной информации;

– сканирование с использованием программ, последовательно перебирающих возможные точки входа в систему (например, номера TCP-портов или телефонные номера) в целях установления путей и возможностей проникновения;

– подмену, навязывание, уничтожение, переупорядочивание или изменение содержимого данных (сообщений), передаваемых по сети, и др.

Одной из ключевых проблем, связанных с доказыванием вины обвиняемых, является невозможность вменить подозреваемым организацию преступного сообщества, т. к. преступная деятельность, ведущаяся в электронных сетях, не предполагает личного знакомства злоумышленников. В связи с этим органам следствия становится невозможным отразить все признаки, указанные в УК РФ, – устойчивость, распределение преступных ролей и т. д. Кроме того, не следует забывать, что доходы от киберпреступности настолько высоки, а специалисты в этой сфере преступной деятельности настолько ценны, что на их физическую и юридическую защиту тратятся серьезные средства, что существенно ограничивает доступ правоохранителей к этим лицам [4, с. 94-96].

Такое положение формирует повышенный интерес у идеологически незрелых слоев населения, в особенности у подростков, из которых рекрутируются новые члены преступных сообществ через сеть «Интернет», используя форумы в социальных сетях, подростковые сайты знакомств, такие как «Галактика», «Фанфик.ру» и т. п., формируя мировоззрение через фан-встречи с блогерами рунета: Ивангай (12,2 млн подписчиков, 315 публикаций на youtube.com), Ян Го, Марьяна Ро, Саша Спилберг, Катя Клэб, даже через силлабо-музыкальные композиции антисоциальной направленности таких исполнителей, как Фейс (1,2 млн подписчиков, 342 подписки, 45 публикаций – в Instagram), Тони Раут (148,7 тыс. подписчиков, 275 подписок, 660 публикаций – в Instagram), Оксимирон (1,7 млн. подписчиков, 295 подписок, 1,578 публикаций – в Instagram), Джоннибой (32,9 тыс. подписчиков, 41 подписок, 142 публикаций – в Instagram) т. п., выкладываемые в сети.

Современная медицина, психологическая и педагогическая наука считают, что мозг ребенка (подростка), в частности ряд его структур, расположенных на обеих сторонах таламуса, непосредственно конечного мозга, промежуточного мозга (диэнцефалона) и среднего мозга (мезэнцефалона), более восприимчив к освоению новых технологий, чем мозг взрослого человека, т. к. организация кратковременной и долговременной памяти, в том числе пространственной, организация ориентировочно-исследовательской деятельности лучше структурирована в мозгу подростка, молодой мозг более способен к овладению комплексными специальными познаниями в области новых компьютерных программ и возможностей как конструктивных, так и деструктивных, вредоносных. В связи с этим необходимо подвести идеологи-

ческую базу, квалифицированно направить применение потока этих новых знаний в оптимальное русло, повышая сознательность подрастающего поколения, вырабатывая привычку лояльности к закону.

Лимбическая система головного мозга, отвечающая за выработку желаний нижнего уровня (голод, жажда, половое влечение), а также эмоций и оперативной памяти подростка, начинает формироваться с 11–12 лет, в то время как кора головного мозга, отвечающая за контроль над эмоциями и желаниями, окончательно развивается только к 17–18 годам. Таким образом, возникает опасность развития в этот период патологических наклонностей к стяжательству и нарушению неприкосновенности личной и общественной собственности – воровству, в том числе воровству с использованием новых компьютерных технологий.

Понимая всю важность и повышенную общественную опасность преступлений в сфере компьютерной безопасности, автор видит решение указанных выше проблем в тесном взаимодействии правоохранительных органов Российской Федерации как с федеральными государственными общеобразовательными учреждениями, так и с общественными организациями, занимающимися проблемами современной молодежи [5, с. 131]. Причем речь идет не о формальном сотрудничестве, а о взаимной квалифицированной консультации педагогов, психологов и сотрудников правопорядка. Актуальные вопросы могли бы освещаться сотрудниками органов внутренних дел на круглых столах в средних общеобразовательных учреждениях с участием педагогов, школьного актива, учеников кадетских классов, родителей и других представителей референтных групп подростков. Дальнейшее реформирование уголовного и уголовно-правового законодательства Российской Федерации в части, касающейся киберпреступности, должно своевременно доводиться до широких слоев молодежи. Вопрос правовой информированности населения, в том числе молодежи, должен входить в первостепенные вопросы по выработке единой государственной политики по обеспечению кибербезопасности.

Библиографический список

1. По данным сайта Генеральной прокуратуры Российской Федерации // [Электронный ресурс] https://genproc.gov.ru/smi/news/events/news-864385/ (дата обращения: 25.01.2018).

2. Газета.ру [Электронный ресурс] // МВД России задержало 20 хакеров, заразивших миллион смартфонов https://www.gazeta.

ru/tech/2017/05/ 22/ 10685573/twenty_hackers_apprehended (дата обращения: 25.01.2018).

3. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ: 15.02.2008) [Электронный ресурс] // http:// www.consultant.ru/document/cons_doc_LAW_99662.

4. Попенков А. В. К вопросу о государственном регулировании права арестованного обвиняемого на участие в гражданско-правовых сделках // Уголовно-процессуальный кодекс Российской Федерации: 15-летний опыт применения : сборник научных трудов межведомственной конференции: научное электронное издание. – 2017. С. 94–96.

5. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

К. Р. Аветисян[1]

К ВОПРОСУ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ВОЗДЕЙСТВИЙ

Подходя к информационным аудиальным воздействиям на участников массовых мероприятий с позиции нормативно-правового регулирования заметим, что сам вопрос о предмете нормативного регулирования остается в определенной мере дискуссионным. Основные разногласия могут сводиться к тому, «на какие именно общественные отношения (производственные, идеологические, волевые и т. д.) и на что непосредственно в самих общественных отношениях могут оказывать регулирующие воздействия нормы права» [1].

Из поведения людей, их различных и многочисленных поступков складываются индивидуальные или, как принято говорить, конкретные общественные отношения, которые в свою очередь образуют в качестве «равнодействующей» систему общественных отношений. Важно выяснить, что же подвергается непосредственному правовому регулированию: отдельные конкретные отношения, виды конкретных отношений или вся совокупность общественных отношений в целом.

[1] Преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий МосУ МВД России имени В.Я. Кикотя. © Аветисян К. Р., 2018.

Правовые нормы охватывают непосредственные результаты деятельности, поступков и поведения людей, а не их конечный итог. Они определяют тот или иной вариант поведения при соответствующих условиях и обстоятельствах.

Можно согласиться с мнением, что «предметом нормативно-правового регулирования являются конкретные общественные отношения, а не вся их совокупность» [2].

В общих чертах механизм правового регулирования выделяет потенциальных субъектов правоотношений, определяет их признаки в специальных нормах, указывает на обстоятельства, с которыми связывается действие юридических норм, определяет варианты возможной деятельности.

На нормативном уровне предусмотрено применение информационно-психологического воздействия в практике правоохранительных органов, выраженного непосредственно в аудиальном воздействии с помощью специальных средств. Согласно ч. 2 ст. 21 Федерального закона «О полиции» сотрудник полиции имеет право применять световые и акустические специальные средства:

– для задержания лица, если это лицо может оказать вооруженное сопротивление;

– для освобождения насильственно удерживаемых лиц, захваченных зданий, помещений, сооружений, транспортных средств и земельных участков;

– для пресечения массовых беспорядков и иных противоправных действий, нарушающих движение транспорта, работу средств связи и организаций;

– для защиты охраняемых объектов, блокирования движения групп граждан, совершающих противоправные действия [3].

Применение акустического воздействия может осуществляться при проведении оперативно-разыскных мероприятий, осуществляемых с помощью гласных и негласных методов.

Исходя из анализа нормативных основ информационно-психологического воздействия, мы можем констатировать о фрагментарности правового регулирования и отсутствии специального закона или комплекса норм, системно регулирующих условия и пределы информационно-психологического, включая аудиальное, воздействия.

Применение информационно-психологического воздействия без согласия лица, в отношении которого оно применяется, предполагалось:

– в чрезвычайных ситуациях, возникающих во время катастроф природного, техногенного и антропогенного происхождения в целях локализации и ликвидации последствий чрезвычайных ситуаций;

– при проведении антитеррористических и миротворческих операций, в ходе военных действий при отражении внешней агрессии по отношению к государству.

Проект федерального закона «Об информационно-психологической безопасности» имел существенные недостатки в части юридической техники, что нашло отражение в заключении правового управления нижней палаты парламента [4]. В заключении отмечено, что название и содержание законопроекта не находятся в полном согласовании, поскольку в тексте законопроекта говорится о защите физических лиц, о защищенности отдельных лиц и (или) группы лиц, населения от негативных информационно-психологических воздействий, о воздействии на человека или группу лиц, осуществляемом с использованием специальных средств и методов на психику человека, о субъектах, подвергшихся информационно-психологическому воздействию, об обеспечении информационно-психологической безопасности.

Также во многих статьях законопроекта используются выражения и термины, не имеющие юридического содержания, например, «… осуществляется государством в лице … органов государственной власти, органов местного самоуправления», «негативное информационно-психологическое воздействие», «негативные последствия для психики человека», «утрата способности к … нравственной самоидентификации человека», «блокирование на неосознаваемом уровне свободы волеизъявления человека», «манипуляция общественным сознанием», «традиционные устои общества», «духовное пространство» «экспорт и импорт методов…».

В 2001 г. в связи с отзывом субъектом права законодательной инициативы Советом Государственной Думы было принято решение снять законопроект с рассмотрения Государственной Думы.

В этот же период была предпринята еще одна попытка нормативного регулирования информационно-психологического воздействия. Так, в Государственную Думу был представлен проект федерального закона «О безопасности психосферы человека» [5]. Согласно законопроекту объектами защиты психосферы человека являются психическое здоровье человека, психика и информационные потоки, обеспечивающие функционирование психики человека, дееспособность и

прогрессивное развитие личности, определяющие возможность реализации человеком своих конституционных прав и свобод.

Данный законопроект также получил отрицательное заключение правового управления и был снят с рассмотрения Государственной Думы в связи с отзывом субъектом права законодательной инициативы.

Таким образом, вопросы информационно-психологического воздействия до сих пор не находятся в системном правовом регулировании и неполноценно отражены в законодательстве.

В рамках правоотношений устанавливается конкретная юридическая связь между субъектами, при этом субъекты вполне определенно разделяются на управомоченных и обязанных. Именно здесь выявляется, какая из сторон правоотношения имеет интерес и соответствующие субъективные права, а какая обязана не препятствовать удовлетворению этого интереса либо осуществлять конкретные активные действия в интересах управомоченного.

Нормы права в совокупности с юридическими фактами образуют конкретные правила поведения для участвующих в правоотношениях субъектов.

В случаях, когда на данной стадии имеются препятствия для реализации прав и обязанностей, то возникает необходимость в четвертой стадии, носящей факультативных характер, а именно: в контроле над использованием прав и исполнением обязанностей или защиты прав и интересов субъектов правоотношений.

Полагаем возможным выделить целенаправленное информационно-психологическое воздействие как объект правового регулирования, включающий в себя социальные связи, то есть собственно общественные отношения, между их субъектами, находящимися под воздействием («внутри») механизма правового регулирования, их поведение, действия или бездействие.

Нормативная основа должна создать условия для развития организационной составляющая информационно-психологических воздействий, определить структуру и функции институтов публичной власти и гражданского общества, задействованных в данном направлении, что будет непосредственно содействовать реализации положений Доктрины информАционной безопасности Российской Федерации. Кроме того, в рамках надлежащего нормативного регулирования свое развитие должна получить технологическая составляющая, способствующая свободному и безопасному информационному обмену внутри общест-

ва, содействовать предотвращению и предупреждению угроз информационно-психологической безопасности.

Формирование нормативных основ позволит обеспечивать надлежащую институционализацию информационно-психологического воздействия как объекта правового регулирования в дальнейших стадиях рассматриваемого механизма, предусмотреть условия для привлечения к ответственности за общественно опасное информационно-психологическое воздействие.

Целенаправленное информационно-психологическое воздействие как объект правового регулирования носит неполноценный, фрагментарный характер. В виду отсутствия системного нормативного закрепления и охраны прав и законных интересов участников общественных отношений, связанных с информационно-психологическим, в том числе аудиальным, воздействием, механизм правового регулирования требует дальнейшей разработки в теоретическом и практическом плане. В практическом плане, в первую очередь, на законодательном уровне.

Библиографический список

1. Шейндлин Б. В. Механизм административно-правого регулирования. – СПб., 1961. URL: http://law.edu.ru.

2. Горшенев В. М. Способы и организационные формы правового регулирования в социалистическом обществе. – М. : Юрид. лит., 1972.

3. Заключение правового управления Государственной Думы Федерального Собрания Российской Федерации на проект федерального закона «Об информационно-психологической безопасности».

4. Заключение правового управления Государственной Думы Федерального Собрания Российской Федерации на проект федерального закона «Об информационно-психологической безопасности».

5. Проект федерального закона «О безопасности психосферы человека».

А. М. Голубкина [1]

ЭМОЦИИ ЧЕЛОВЕКА: ВОЗМОЖНОСТИ ПРОВЕРКИ ИСКРЕННОСТИ

Психология эмоций как наука едва достигла своего совершеннолетнего возраста. Эта довольно актуальная тема имеет неотъемлемое значение для человеческой самооценки и социальных взаимоотношений. Существует много взглядов на природу, возникновение и значение эмоций. Даффи считает, что поведенческие проблемы легче объяснить с помощью таких понятий, как «активация» или «стимуляция». Другие утверждают, что эмоции формируют систему мотиваций человека. Некоторые считают, что эмоции являются краткосрочным состоянием, и, напротив, существует мнение, что для человека естественно быть подвергнутым воздействию одной и той же эмоции на протяжении длительного времени. Кроме того, есть два противоположных взгляда о влиянии эмоций на поведение человека: эмоции могут разрушать человеческое поведение и являются одной из причин многих психических заболеваний, либо эмоции являются своего рода позитивным организатором в мотивации и укреплении поведения [1].

Психологи, а также философы и педагоги не имеют единой точки зрения относительно роли, которую эмоции играют в жизни человека. Некоторые из них утверждают, что смысл человеческого существования должен быть ограничен познавательно-интеллектуальной деятельностью, в то время как другие ученые убеждены, что данный смысл имеет эмоциональную основу, поскольку для человека естественно строить свое окружение из таких людей и вещей, к которым он привязан на эмоциональном уровне.

Маурер один из первых, кто выразил важную роль эмоций в основе человеческого поведения, утверждая, что эмоции являются одним из наиболее важных факторов в изменении поведения или его результатов, которые принято называть научением.

Отечественные психологи убеждены, что эмоции – особая форма отношения к объектам и явлениям реальности, выделяя при этом три аспекта этих процессов: первый аспект переживания (С. Л. Рубинштейн, Г.С. Шингаров); второй аспект отношения (П. М. Якобсон, В. Н. Мясищев); третий аспект отражения (В. К. Вилюнас, Ю. М. Веккер, Г. А. Фортунатов).

---

[1] Курсант 234 учебного взвода Института психологии служебной деятельности ОВД МосУ МВД России имени В.Я. Кикотя. © Голубкина А. М., 2018.

С первой точки зрения специфика эмоций – это опыт событий и отношений. С. Л. Рубинштейн считал, что чувства выражают себя в форме познания отношения субъекта к окружающей среде, к тому, что он знает и делает. С другой стороны, как упоминали в своих исследованиях А. В. Запорожец и Я. З. Неверович, эмоции играют ключевую роль в реализации этих мотивов. Они считают, что эмоции – это не просто процесс активации, а особая форма отражения субъектом реальности, посредством которого происходит ментальный контроль активации, а точнее, что происходит психическая регуляция общего направления и динамики поведения. Ряд авторов (Г. Х. Шингаров, Г. И. Батурина и др.) считают, что основа для различия эмоций и чувств как качественно отличных психических явлений эмоциональной сферы обусловлена рядом критериев. Во-первых, потребностями, которыми эти явления обусловлены, во-вторых, функциями, которые они выполняют, в-третьих, физиологическими механизмами, с помощью которых они обусловлены.

Эмоции – это психические процессы, в которых человек испытывает свое отношение к определенным явлениям окружающей действительности. Эмоции также отражают различные состояния человеческого тела, его отношение к собственному поведению и своей деятельности.

Без развития психологических характеристик личности, таких как сензитивность, эмоциональная устойчивость, экспрессивность, чувствительность, невозможно представить процесс формирования коммуникативной компетентности специалистов правоохранительных органов [2].

Подходы к формированию коммуникативной способностей личности через развитие релевантных индивидуально-психологических характеристик, относящихся к эмоциональной сфере специалиста, рассмотрены в ряде работ авторов [3].

Эмоции необходимы для выживания и благополучия людей. Без эмоций люди бы не обладали всем спектром человеческих качеств. Эмоции стали ключевым признаком человечности. Не менее важна наша способность сопереживать эмоциям других людей, способности к эмпатии и умению выражать эмоции в словах, говорить о них. Важным критерием для таких эмоций является искренность.

Искренность говорящего – понятие, хорошо известное в повседневной жизни при осуществлении межличностных отношений и плохо понимается в психологической науке. Не случайно, что термин

«искренность» отсутствует в словаре «Психология» (1990) и «Большом психологическом словаре» (2005), опубликованном под девизом «Главная книга по психологии». В обществе искренность воспринимается как положительное качество говорящего, как этическая и даже эстетическая норма речевого поведения. Об этом свидетельствуют многие известные произведения, начиная с учений Конфуция («Благородный муж должен видеть, искренна ли его речь...») и заканчивая словарями В. Даля и С. И. Ожегова: «искренний – правдивый, откровенный, честный, добросовестный, выражающий подлинные чувства, чистосердечный, нелицемерный и т. д.» [4].

В психологии, в том числе социальной, искренность считается эффективным средством общения и влияния на общественность и связана с терминами «истина», «ложь», «правда», «правдивость», включая проблему лжи, которая просматривается через невербальные свойства. В юридических работах, как и в социологии, термин «искренность» является синонимом правдивости (Коченов, Ефимова, Кривошеев, Ситковская, 1987), т. е. напрямую связано с личностью говорящего.

Повышение профессионализма сотрудников ОВД и эффективности их деятельности, предусматривает не только совершенствование нормативно-правовой базы, организации и технологических приемов деятельности, но и активизацию «человеческого фактора», постоянное совершенствование профессиональной компетентности, в т.ч. и психологических характеристик сотрудников ОВД [5].

Профессиональная этика требует от сотрудников ОВД постоянно следить за своим поведением, чувствами и эмоциями, не затрагивая личную симпатию или антипатию, неприязнь, плохое настроение или чувства дружбы, чтобы влиять на официальные решения, способные предвидеть последствия своих действий. Но под влиянием человеческих эмоций рождаются скоординированные сокращения и расслабления различных лицевых структур. Они определяют выражение, которое прекрасно отражает переживаемые эмоции. Поскольку состояние мышц лица легко контролировать, его часто пытаются маскировать и даже имитировать эмоции в лицо. Знание мимики с разными эмоциями полезно не только для понимания других, но и для тщательной доработки своих имитационных работ.

Как можно установить искренность сотрудника ОВД? Остановим акцент на невербальных способах. Честно говорят о внутренних переживаниях человека его глаза. В процессе общения люди часто смотрят друг другу в глаза, когда слушают, а не когда говорят, хотя ино-

гда, когда необходимо прибегнуть к внушению, они человек смотрит прямо в глаза своему партнеру [6].

Модификации контактов глаз имеют следующую расшифровку:

– отсутствующий взгляд – сосредоточенное размышление;

– переведение взгляда на окружающие предметы и в потолок – падение интереса к беседе, излишне длинный монолог партнера;

– настойчивый и пристальный взгляд в глаза (зрачки сужены) – признак враждебности и явного желания доминировать;

– настойчивый и пристальный взгляд в глаза (зрачки расширены) – знак сексуальной заинтересованности;

– отвод и опускание взгляда – стыд, обман;

– взгляд сбоку – недоверие;

– взгляд то отводится, то возвращается назад – отсутствие согласия, недоверие.

Важную информацию о внутреннем настроении человека дает статическое положение его тела. В этом случае часто повторяющиеся позы сообщают об устойчивых характеристиках личности. Поскольку лицевые мышцы обычно лучше контролируются при перепадах чувств, чем тело, часто ключевым в определении искренности является не выражение лица собеседника, а поза, способная сообщить об истинных переживаниях. Не забудьте о жестах. «Жест – это не движение тела, а движение души». Он говорит о желании человека и о том, что он переживает в тот момент, а жест, вошедший в привычку, указывает на характер своего обладателя.

Несмотря на то, что на данный момент существует множество способов разоблачения лжи, ни один из них нельзя назвать универсальным. Невербальные средства передачи информации, на наблюдении за которыми базируется большинство теорий и методик выявления лжи, достаточно субъективны.

Библиографический список

1. Изард К. Э. Психология эмоций. – СПб. : Питер, 2007. – С. 15.

2. Здорова С. В. Исследование психологических факторов, влияющих на формирование компонентов коммуникативного потенциала курсантов образовательных учреждений МВД России // Вестник Московского университета МВД России. – 2011. – № 3. – С. 25–31.

3. Сударик А. Н., Здорова С. В. Подход к формированию коммуникативных способностей обучающихся в рамках учебного процесса на факультете подготовки психологов // Международный журнал психо-

логии и педагогики в служебной деятельности. – 2016. – № 1. – С. 100–102.

4. Здорова С. В., Сударик А. Н. Формирование коммуникативных способностей обучающихся при проведении практических занятий по дисциплине «Общий психологический практикум»: технологический подход // Человеческий фактор: проблемы психологии и эргономики. – 2016. – № 1 (77). – С. 80–81.

5. Морозов В. П. Невербальная коммуникация. Экспериментально-психологические исследования. – М. : ИП РАН, 2011. – С.18.

6. Сударик А. Н. Профессиональная компетентность сотрудников ОВД и некоторые ее психологические составляющие в свете подготовки специалистов в педагогической системе МВД // Человеческий фактор: проблемы психологии и эргономики. – 2009. – № 4. – С. 104–105.

7. Федотов С. Н., Кравченко А. В., Осипова А. С. К вопросу о развитии эмоционального интеллекта сотрудников силовых структур // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской Таможенной Академии. – 2017. – № 1 (61). – С. 106–108.

С. Ю. Капицын[1], А. Б. Менисов[2], И. А. Шастун[3]

МЕТОДИКА ОЦЕНИВАНИЯ РЕЗУЛЬТАТИВНОСТИ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

В настоящее время информационное воздействие (ИВ) является одним из основных способов достижения политических, экономических и военных целей.

Информационное воздействие – динамический целенаправленный процесс преобразования передаваемой информации от источника воздействия к целевой аудитории для решения задач изменения у последней мнений, состояний, активности.

В настоящее время наиболее результативное ИВ проводится следующими способами [3]:

– агитацией и пропагандой в реальном мире;

[1] Преподаватель Военной Академии Генерального Штаба. © Капицын С. Ю., 2018.
[2] Адъюнкт Военно-космической академии имени А. Ф. Можайского. © Менисов А. Б., 2018.
[3] Преподаватель Военно-космической академии имени А. Ф. Можайского. © Шастун И. А., 2018.

– распространением материала пропагандистской направленности в сети «Интернет» (deepWeb);

– блоггингом на отдельных сайтах;

– агитацией и пропагандой в социальных сетях.

Развитие сетевых технологий и, в частности, социальных сетей повышает результативность проведения мероприятий по информационному воздействию (в целях достижения (удержания) информационного превосходства). В связи с этим возросло значение информационной деятельности, направленной на создание соответствующих методик и инструментариев, повышающих качество противодействия материалам ИВ. Особое внимание необходимо уделять на стадию оценивания информационного воздействия на целевую аудиторию в социальных сетях.

В социальных сетях ИВ проводится в форме:

– динамической картинки воздействия (видеопропаганды на YouTube каналах и в тематическом потоке);

– статической картинки воздействия (графической пропаганды в Instagram);

– манипулятивной текстовой информацией (текстовой и вышеизложенной формы пропаганды в Вконтакте, Одноклассники, Twitter, Facebook).

Оценивание информационного воздействия – процесс определения значения ожидаемого эффекта информационного воздействия на целевую аудиторию социальных сетей.

Разработанная методика оценивания информационного воздействия предназначена для измерения результативности и получения оценки уровня информационного воздействия на целевую аудиторию и содержит следующие этапы:

Этап 1. Определение параметров реакции целевой аудитории социальных сетей на информационное воздействие в форме манипулятивной текстовой информации.

Взаимосвязь параметров целевой аудитории, материала и группы (источника) в социальной сети представлена на рис. 1.

Рис. 1. Взаимосвязь выбранных параметров социальных сетей

Исходя из опыта оценивания и прогнозирования результатов информационного воздействия посредством интернет-СМИ, а также на основе проведенных экспериментов наиболее информативными являются следующие параметры активности целевой аудитории при информационном воздействии: число подписчиков, охват целевой аудитории, прирост подписчиков, число подписавшихся, число отписавшихся, охват подписчиков, просмотры и переходы на источник.

Этап 2. Определение критериев взаимосвязи параметров реакции целевой аудитории социальных сетей.

При обработке 864 групп в социальной сети «Вконтакте» за один сутки было вычислено вероятностное распределение значений параметров и представлено на рис. 2. Таблица 1 отражает корреляцию параметров целевой аудитории и параметров ИВ при проведенном информационном воздействии и содержит доказанные статистические гипотезы по коэффициенту корреляции Пирсона и p-значении.

Этап 3. Оценка результативности ИВ в социальных сетях.

У оценки результативности ИВ в социальных сетях есть две составляющие: оценка реакции целевой аудитории на сообщество или публичную страницу, на которых размещают материал, воздействующий на объект, и оценка реакции пользователей на данный материал. Расчет комплексного показателя результативности ИВ на целевую аудиторию проводится с использованием следующего выражения:

$$V = \left\{ V_{Ist}, V_M \mid V_{Ist} = (V_{Ist}{}^R, V_{Ist}{}^{RS}, V_{Ist}{}^S); V_M = (V_M^R, V_M^L, V_M^C) \right\}, \quad (1)$$

где:

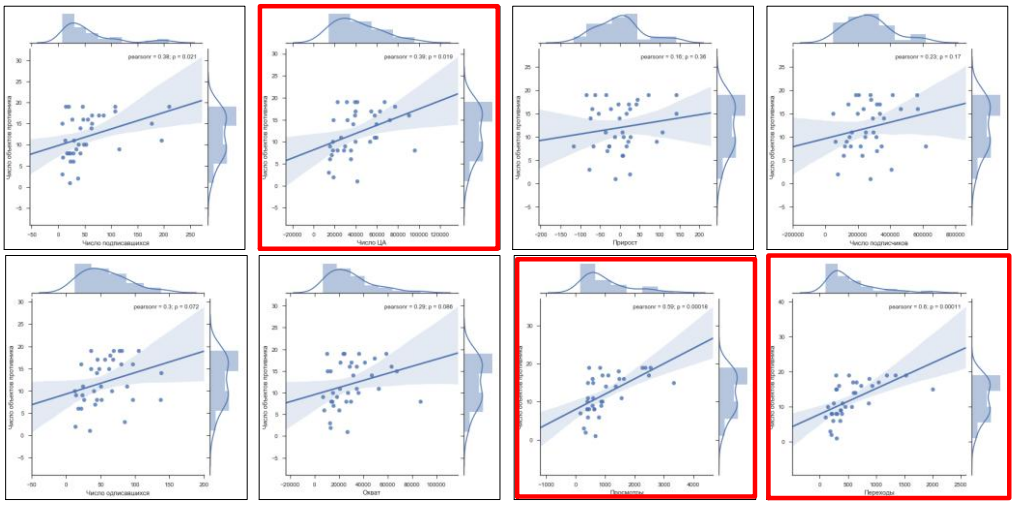


Рис. 2. Распределение параметров

Таблица 1.

Суммарные значения параметров целевой аудитории

День	Дата	Количество просмотров	Количество уникальных посетителей	Полный охват	Охват подписчиков	Число новых подписчиков	Число отписавшихся
1	2016-04-09	25984	13263	452284	365712	635	400
2	2016-04-08	26282	13647	470462	378545	630	361
3	2016-04-07	27824	14624	473696	382254	746	444
4	2016-04-06	28725	14866	490803	394676	787	419
5	2016-04-05	28565	14641	491865	392539	764	453
6	2016-04-04	28469	14610	499187	389017	757	433
7	2016-04-03	31597	15605	490768	388797	865	494

$V_{Ist}^{R} = \dfrac{охват\ ЦА}{количество\ подписчиков}$ – определяет охват общей целевой аудитории;

$V_{Ist}^{RS} = \dfrac{охват\ ИВ}{общее\ количество\ просмотров}$ – определяет охват ИВ;

$V_{Ist}^{S} = \dfrac{прирост\ подписчиков}{общего\ количества\ переходов}$ – прирост целевой аудитории;

$V_{M}^{R} = \dfrac{количество\ заимствования}{количество\ просмотров\ спец.\ материала}$ – распространение материалов ИВ,

$V_{M}^{L} = \dfrac{количество\ отметок\ "мне\ нравиться"}{количество\ просмотров\ спец.\ материала}$ – оценка материалов ИВ;

$V_M^C = \frac{количество\ комментариев}{количества\ просмотров\ спец.\ материала}$ – комментирование материалов ИВ.

Исходя из условий распространения информации в социальных сетях формируется необходимость анализа и обработки информации в большом количестве для осуществления оценивания ИВ.

С помощью предложенной методики было рассмотрено 128 сообществ социальной сети «Вконтакте» одной тематической направленности, показатели за семь суток представлены в табл. 2.

Таблица 2

Суточная результативность ИВ

День	Результативность ИВ	Число привлечения
1	0,453345192	1,5875
2	0,434402776	1,745152
3	0,46420682	1,68018
4	0,45347301	1,878282
5	0,434991845	1,686534
6	0,391022965	1,748268
7	0,462896314	1,751012

В последние годы роль информационной сферы неизменно возрастает. Для информационного воздействия активно задействуются Интернет и СМИ. В данной статье представлена методика оценивания результатов информационного воздействия на пользователей в социальных сетях на основе учета новых критериев расчета изменения показателей активности пользователей. Также в статье представлен комплексный показатель результативности информационного воздействия. В материалах статьи методика оценивания показана на примерах групп социальной сети «Вконтакте».

Библиографический список

1. Гриняев С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны. – Минск : Харвест, 2004. – 448 с.

2. Бобров А. Информационная война: от листовки до твиттера // Зарубежное военное обозрение. – 2013. – № 1. – С. 20–27.

3. Капицын С. Ю., Менисов А. Б., Шастун И. А. История и классификация средств идеологического воздействия // Экономика и социум. – 2015. – Вып. № 1 (14). – Январь-март.

Н. В. Аникеева[1], *А. С. Ропалло*[2]

ПСИХОЛОГИЧЕСКИЙ ПОРТРЕТ ПРЕСТУПНИКА В СЕТИ «ИНТЕРНЕТ»

Интернет давно и прочно вошел в человеческую жизнь. Благодаря возможностям Интернета люди могут общаться друг с другом на расстоянии, покупать товары прямо из дома, делиться фотографиями с помощью электронной почты и социальных сетей, зарабатывать деньги.

В современном мире преступления в сети «Интернет» очень распространены. Преступники не дремлют, так же как в реальной жизни они могут совершать преступления по Интернету, иногда по неосторожности, иногда преднамеренно, зачастую надеясь, что их не смогут найти и наказать.

Но виртуальная жизнь, как и реальная, подчиняется реальным законам, по которым возбуждаются уголовные дела в отношении человека, совершившего преступление в сети «Интернет».

Цифровой мир XXI в. – системное понятие, интегрирующее такие категории, как цифровая среда (пространство), цифровые технологии, цифровое общество, цифровая экономика, цифровое государство и граждане цифрового мира. По статистическим данным в 2017 г. цифровая революция перешла на новый этап – к Интернету подключился каждый второй житель Земли. По оценке Глобального института McKinsey (MGI), уже в ближайшие 20 лет до 50 % рабочих операций в мире могут быть автоматизированы, и по масштабам этот процесс будет сопоставим с промышленной революцией XVIII – XIX вв.

Россия уже живет в цифровой эре: по количеству пользователей Интернета она занимает первое место в Европе и шестое – в мире. За последние три года смартфонов у нас стало вдвое больше – теперь они есть у 60 % населения. Это больше, чем в Бразилии, Индии и странах Восточной Европы [2].

Цифровые преобразования – один из главных факторов мирового экономического роста. По оценкам Глобального института McKinsey, в Китае до 22 % увеличения ВВП к 2025 г. может произойти за счет интернет-технологий. В США ожидаемый прирост стоимости, созда-

---

[1] Преподаватель кафедры психологии УНК ПСД МосУ МВД России имени В.Я. Кикотя кандидат педагогических наук. © Аникеева Н. В., 2018.

[2] Слушатель 433 учебного взвода ФПИС МосУ МВД России имени В.Я. Кикотя, старший сержант милиции Республики Беларусь. © Ропалло А. С., 2018.

ваемый цифровыми технологиями, впечатляет не меньше – здесь он к 2025 г. может составить 1,6–2,2 трлн долл. США.

По оценкам Глобального института McKinsey, потенциальный экономический эффект от цифровизации экономики России увеличит ВВП страны к 2025 г. на 4,1–8,9 трлн руб. (в ценах 2015 г.), что составит от 19 до 34 % общего ожидаемого роста ВВП [2].

Такие экономические прогнозы связаны не только с эффектом от автоматизации существующих процессов, но и с внедрением принципиально новых, новаторских бизнес-моделей и технологий. Среди них – цифровые платформы, цифровые экосистемы, углубленная аналитика больших массивов данных, технологии «Индустрии 4.0», такие как 3D печать, роботизация, Интернет вещей.

Как отмечено в концептуальных документах разных стран (Китай, Малайзия, Боливия, Кения, Россия, Турция, Саудовская Аравия, Бангладеш, Колумбия, ОАЭ, Филиппины, Польша, Мексика, Индонезия, Марокко) – лидеров цифрового мира (согласно рейтингу Digital Evolution Index [3]), важнейшим критерием перехода страны в цифровой мир является всеобщая связанность, интеграция личных девайсов (многофункциональных устройств), общественных сетей, корпоративных систем и правительственных инфраструктур в единое целое – цифровой взаимосвязанный мир. Это, с одной стороны, открывает широкие возможности, но одновременно делает нас обитателями «дома со стеклянными стенами». В данном случае возможности, риски и угрозы растут пропорционально и экспоненциально.

В связи с этим, исследование психологических особенностей личности интернет-преступника в современной действительности является актуальным и своевременным.

Предметом настоящего исследования является теоретический анализ проведенных исследований по теме, данные психологических опросов пострадавших, дополняющие характеристику личности современного интернет-преступника.

Целью исследования – психологический анализ наиболее важных личностных характеристик преступника в сети «Интернет».

Социальная инженерия – совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним. Вместе с тем в современном мире используется и второе значение этого термина – манипулирова-

ние людьми, а не машинами, в целях проникновения в защищенные системы предприятия или потребителя.

Социальный инжиниринг является способом совершения компьютерных преступлений.

Статистика причин информационных угроз, представленная компанией Gartner Group[1], говорит о том, что человеческий фактор (55 %) занимает значительную долю от общего числа причин информационных атак (рис. 1).

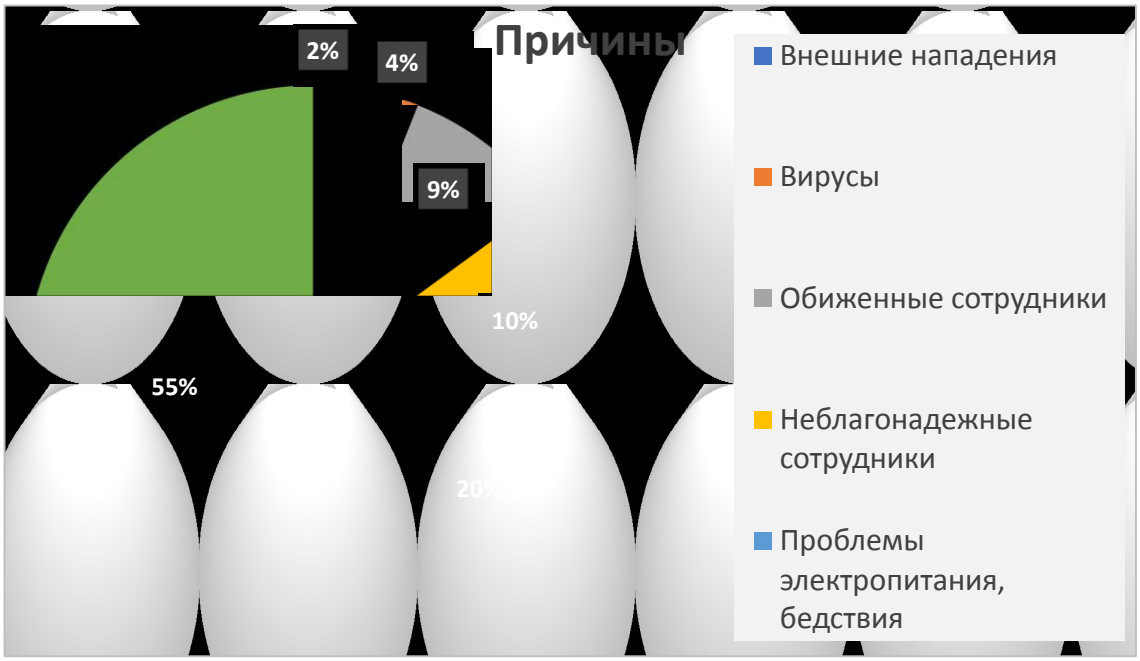


Рис. 1. Причины информационных атак

У каждого современного человека можно найти уязвимые стороны, поразить которые становится задачей интернет-преступника, стремящегося использовать социальную инженерию в своих преступных целях.

При этом можно выделить некоторые из психокомплексов [4], присущих любому человеку вне зависимости от пола, возраста, социального статуса, социальной роли, материального благополучия и других факторов, которые применяются злоумышленниками: страх; любопытство; жадность; превосходство; великодушие и жалость; доверчивость.

В мире ежегодно регистрируется огромное количество киберпреступлений, среди которых [1]:

[1] Исследовательская и консалтинговая компания, специализирующаяся на рынках информационных технологий.

Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ (хакерство, взлом шифра). незаконное получение данных (информационный шпионаж), незаконный перехват, искажение информации, искажения системы).

Преступления, связанные с контентом (расизм, агрессивные высказывания, восхваление жестокости, религиозные преступления, незаконные азартные игры и онлайновые игры, клевета и фальшивая информация, спам и связанные с ним угрозы, вымогательство, другие формы незаконного контента).

Преступления, связанные с правами собственности и товарными знаками (преступления, связанные с авторскими правами, преступления, связанные с товарными знаками).

Преступления, связанные с применением компьютеров (мошенничество и компьютерное мошенничество, подлог, связанный с применением компьютеров, кража идентичности, неправомерное использование устройств).

Комбинированные преступления (отмывание денег с использованием компьютерных технологий, фишинг).

Проведенный нами опрос при помощи социальной сети «Вконтакте» показал, что наиболее распространены следующие виды преступлений в Интернете.

Создание, распространение и использование компьютерных программ, причиняющих вред компьютеров (100 %). Это различные вирусы и так называемые «черви», которые цепляются компьютером при выходе в Интернет. Они зачастую маскируются под полезные и нужные, а на самом деле портят всю компьютерную систему, вызывая сбои и торможения, а также похищая данные пользователя.

Нарушение авторских прав (100 %). Преступники крадут у автора его продукт, а затем распространяют без его ведома.

Попрошайничество в Интернете (94 %). На почтовый адрес пользователя доставляется письмо с призывом о помощи от благотворительных организаций или людей, оказавшихся в беде. Такие письма содержат данные реальных фондов и людей, но реквизиты предоставляются мошенниками. На самом деле такие организации не занимаются рассылкой писем пользователям, они пользуются другими методами. Пользователь может найти телефон указанной организации, позвонить туда и спросить о том, каким образом им можно перечислить деньги.

Уведомления о выигрыше (92 %). Этот вид преступления заключается в том, что на е-мэйл пользователя присылается письмо о том, что он будто бы получил приз в виде крупной суммы или автомобиля. Мошенники пытаются выманить у пользователя определенную сумму денежных средств будто бы для получения его выигрыша. Она может колебаться от нескольких сотен до нескольких тысяч. По словам преступников, это налог на приз. Пользователь должен заподозрить неладное, т. к. он не принимал участия в каких-либо лотереях, в которых мог бы что-то выиграть. Если потерять бдительность и не заметить преступления через Интернет, то можно понести большую потерю в виде денег, тогда придется прибегать к помощи юриста.

Письма от мошенников (82 %) являются преступлениями по Интернету, их трудно отличить от настоящих, т. к. они научились подделке своих писем под сообщения от различных официальных организаций, на консультации у юриста об этом можно узнать подробнее. Ими применяются и логотипы компаний, и стиль написания. В таких письмах содержится ссылка с просьбой перейти по ней для того, чтобы пользователь ввел свои реквизиты, будто бы для своей безопасности. Ничего не подозревая, пользователь переходит на сайт, который трудно отличить от настоящего, и вводит там свои данные. После чего преступники получают доступ к его счету, а пользователь попадает на их настоящий сайт.

Создание групп смерти (49 %). Период от возникновения суицидальных мыслей до попытки их реализации называют пресуицид: индивид находится в состоянии угнетающего аффекта, его мрачные мысли усиливаются, неудовлетворенность жизненными условиями растет. Материалы, размещенные на личных страницах в социальных сетях участников виртуальных клубов самоубийц, показывают, что они испытывают депрессию и страдают от одиночества. Такое настроение является благоприятной почвой для внушения и развития угнетающего настроения, характерного для пресуицидального периода.

Кардинг (47 %) – вид преступления в сети «Интернет», представляющий способ мошенничества с банковскими картами. Мошенниками производится похищение банковских реквизитов карты с помощью взлома серверов интернет-магазинов, систем платежей или с персонального компьютера пользователя.

Интернет-аукционы (42 %). Продавцы выставляют товар на аукцион, но для повышения ставок используют ботов либо повышают их

сами, чтобы пользователь не смог купить выставленный товар подешевле.

Фишинг (37 %) – это очень серьезное преступление через Интернет. Это такие уведомления, отправленные якобы администраторами систем платежей или от банка, почтовых серверов или из соцсетей. В этих уведомлениях содержатся призывы пройти по указанной ссылке, чтобы украсть учетные данные пользователя в виде логина и пароля. Целью таких манипуляций может быть счет в банке, учетная запись в платежных системах, электронная почта и социальные сети. Как только мошенники получают то, что им нужно, то они быстро применяют это для доступа к счету банка пользователя.

Неправомерный доступ к компьютерной системе (26 %). Взлом компьютерной системы для того, чтобы заполучить информацию, распространить ее или удалить.

Нарушение правил эксплуатации, средств хранения, обработки или передачи охраняемой информации, или компьютерных сетей и оборудования, и правил доступа, которое повлекло за собой то, что информация была уничтожена, блокирована, модифицирована либо копирована, что причинило большой урон (26 %).

Педофилия (19 %) и распространение детской порнографии. Преступник может войти в доверии к ребенку через соцсети, попросить его о личной встрече, а затем за вознаграждение совершить либо действия сексуального характера, либо незаконную фотосъемку, а затем распространить снимки по Интернету либо выставить их на специальный сайт.

Нигерийский спам (17 %). Довольно старая схема мошенничества в сети «Интернет». Пользователь получает письмо, где автор письма заявляет, что у него есть миллионы долларов, которые были выручены не совсем честными методами, поэтому ему нужно вывести деньги за рубеж. Автор просит пользователя помочь ему в обналичивании крупной суммы денежных средств, обещая за услугу несколько процентов от этой суммы. Целью такого мошенничества является то, что пользователь предоставит свой счет в банке, на котором в скором времени благодаря мошенникам не останется средств [5].

Результаты опросов и беседа с потерпевшими также определили, что крайне большой вред им и их близким был нанесен: взломом почты и социальной сети, переводом денег, рекламой с содержанием порнографии, вымогательством.

Однако на вопрос «Знаете ли вы о мере ответственности, наступающей за преступления такого рода?», лишь 10% респондентов ответили положительно. Это в очередной раз показывает достаточно высокую латентность интернет-преступлений.

Несмотря на высокий интерес к предложенной нами теме, отдельные исследования личности компьютерного преступника в общем и интернет-преступника присутствуют – однако они либо не полные, либо устарели в связи с быстрым изменением характеристики показателей состояния и структуры интернет-преступности.

Проанализировав большой массив литературы, практических исследований по данному вопросу, проведя соцопрос, нами был составлен обобщенный психологический портрет личности преступника в сети «Интернет». При составлении портрета учитывались социально-демографические признаки личности преступника, такие как пол, возраст, наличие судимостей, его нравственно-психологические характеристики, мотивация, установки на посещение сайтов определенной направленности в Интернет, отношение к совершенному деянию, среда проживания и т. д.

Анализ работ В. Н. Кудрявцева, Т. П. Кесаревой показал следующее:

Распределение преступников по гендерному признаку: 97,2 % – мужчин и лишь 2,8 % женщин.

Распределение преступников по возрасту выглядит следующим образом: до 18 лет – 29,9 %; от 18 до 24 лет – 60,4 %; старше 24 лет – 9,7 %. При этом самому младшему 12 лет, самому старшему – 45. Средний возраст преступника около 20 лет.

Постоянное место работы имеют 31,3 % лишь у 13,9 % из выявленных лиц работа связана с обслуживанием компьютеров, программированием и т. д. Обучаются в высших учебных заведениях 38,2 %, 25,7 % – на технических специальностях, так или иначе связанных с компьютером; 14,6 % – подростки, обучающиеся в школах.

Чаще всего лица, ранее не судимы, в свою очередь 84,72 % исследуемых лиц признало свою вину и раскаялось, все из них возместили материальный ущерб; 13,19 % лиц, совершивших интернет-преступления, признали вину частично; 2,08 % отрицали вину, но никто не отрицал свою причастность к преступлению.

Мотивом чаще всего является: корыстные побуждения – 95,83 %; любопытство и исследовательские побуждения – 58,33%; доказатель-

ство собственного превосходства – 22,92 %; желание приобщиться к маргинальной социальной группе – не ниже 18,75 % [6].

Мошенник в сети – всегда лжец, поэтому ему присущи такие свойства (зачастую не врожденные, а приобретенные): конспиративность; закрытость; театрализация действий (он склонен к перевоплощению, причем свои действия не репетирует).

У него зачастую достаточно высокий интеллектуальный уровень, однако в большей степени в криминальном плане: он любит просчитывать варианты, ему это нравится, причем ему надоедает одно и то же, и он ищет креатива, ему хочется быть лидером в своей области, хочется монополизировать свою «тактику». У него гибкое мышление, то есть он может подстраиваться под ситуации, менять стиль поведения, быстро решать проблемы. В то же время ему присущ высокий уровень тревожности [7].

Такая личность изначально идет к деформации, причем это начинается не в сознательном возрасте, а много раньше – в школе и детском саду, когда можно увидеть черты ребенка, склонного ко лжи и воровству. Он идет на это специально – не для того, чтобы избежать наказания, а для того, чтобы что-то совершить. Как правило они люди эгоистичные и замкнутые по своей натуре. Чтобы сдерживать такие социальные качества, им приходится прибегать к алкоголю и наркотикам. Чаще всего они доходят до этого, потому что они понимают свою роль отчужденца, что они социально неприемлемы.

Подводя итоги вышесказанному, хотелось бы обратить внимание на ежегодно растущий уровень интернет-преступности, что в свою очередь свидетельствует о формировании достаточно новой субкультуры интернет-преступников. Данный материал в очередной раз формирует понимание и позицию по отношению к данного рода преступлениям, представляющим значительную угрозу целостности личности, общества и государства.

Библиографический список

1. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. – М. : Норма: ИНФРА–М, 2018. – 352 с.

2. Цифровая Россия: новая реальность: отчет / Digital/McKinsey. Июль, 2017 // URL: https://apptractor.ru/info/analytics/otchyot-tsifrovaya-rossiya-novaya-realnost.html.

3. Digital Evolution Index, Интернет-портал URL: http://hbr-russia.ru/innovatsii/trendy/p23271.

4. Антоненко Н.В. Периодическая система законов психики человека. – М., 2010. – 48с.

5. Овчинский В. С. Криминология цифрового мира : учебник для магистратуры. – М. : Норма: ИНФРА–М, 2018. – 352 с.

6. Кесареева Т. П. Криминологическая характеристика и предупреждение преступности в российском сегменте сети «Интернет» : дис. … канд. юрид. наук. – М., 2002. – С.103.

7. Родкина Е. А., Иванов В. Ю. Некоторые аспекты мониторинга социальных сетей // Технологии информационной безопасности в деятельности органов внутренних дел. – М. : МосУ МВД России имени В.Я. Кикотя, 2016. – С. 86–89.

Д. В. Деулин[1], А. В. Кравченко[2]

ПЕРСПЕКТИВНАЯ ИНСТРУМЕНТАЛЬНО-ПСИХОЛОГИЧЕСКАЯ МЕТОДОЛОГИЯ ВЫЯВЛЕНИЯ СКРЫВАЕМОЙ ИНФОРМАЦИИ В РАМКАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В настоящее время социальная инженерия рассматривается как некая совокупность подходов в прикладных социальных науках, ориентированных на изменение поведения и установок людей, разрешение социальных проблем, адаптацию социальных институтов к изменяющимся условиям и сохранение социальной стабильности [1]. Вместе с тем, отдельные методы социальной инженерии могут быть использованы не на общественное благо, а в угоду частным интересам. Так, в сфере высоких технологий методы социальной инженерии могут быть использованы для незаконного доступа к информации или системам хранения информации без использования технических средств. Сами инструменты социальной инженерии могут быть направлены на изменение поведения человека, его привычного паттерна поведения путем введения в заблуждения или предоставление неточных сведений.

[1] Доцент кафедры психологии учебно-научного комплекса психологии служебной деятельности МосУ МВД России имени В.Я. Кикотя кандидат психологических наук. © Деулин Д. В., 2018.

[2] Старший научный сотрудник учебно-научного комплекса психологии служебной деятельности МосУ МВД России имени В.Я. Кикотя. © Кравченко А. В., 2018.

Социальная инженерия сегодня выступает как особый вид мошенничества с привлечением современных технологий. Прообраз социальной инженерии можно обнаружить в рекламе. Там цель – убедить любыми способами человека в необходимости приобретения рекламируемой продукции, в обосновании чего-либо. Примером может быть применения софистики. Всем известный античный софизм: «У тебя есть то, что ты не терял, ты не терял рога, значит, у тебя есть рога» [2]. В рекламе можно встретить «незавершенный» софизм. Например, для обоснования показа рекламы в московском метрополитене можно перед входом в Интернет прочитать надпись «Пока вы смотрите рекламу – в мире рождается 356 котят». Создается бессознательная установка на одобрение просмотра рекламы, ведь в результате рождаются котята. Цель таких софизмов – ввести в заблуждение слушателя, вызвать положительные эмоции.

Однако это пример непреступного использования социальной инженерии, направленный не на приобретении информации, а, наоборот, на предоставление ненужной информации с целями продвижения продукции и услуг. Существуют более агрессивные формы социальной инженерии, которые воплощаются в современном информационном пространстве. Так, с помощью методов социальной инженерии можно совершать уголовно-наказуемые деяния: «бесконтактные убийства» (синий кит) – поиск психологической информации о пользователях сети с целью довести их до самоубийства. Это могут быть иные преступления, с помощью общения в информационном пространстве приобретая «ключи доступа» к аккаунтам банковских карт злоумышленники совершают хищение денежных средств. Высокие технологии и методы социальной инженерии становятся удобным универсальным орудием преступления. Но компьютерные технологии и методы социальной инженерии представляют опасность только при совмещении их с преступным умыслом.

В целях разоблачения злоумышленников можно использовать современную инструментально-психологическую методологию выявления скрываемой информации. Воздействуя на преступника психологическими стимулами и регистрируя деятельность его физиологических систем, можно анализировать достоверность информации, тем самым определять его предрасположенность к реализации преступного умысла.

Важно отметить, что в настоящее время среди наиболее надежных инструментальных методов выявления скрываемой информации оста-

ется полиграф. Однако развитие науки и техники не оставляет сомнений в том, что в скором будущем будут совершенствоваться технические возможности аппаратных средств диагностики лжи. Кроме того, будут создаваться инновационные методы, основанные на сканирование участков головного мозга в целях фиксации очагов возбуждения в ответ на предъявление значимых стимулов.

Сегодня одной из разновидностей психофизиологического метода выявления лжи является анализатор стресса по голосу. Данный метод основа на том, что происходит регистрация изменений динамики речевого сигнала в ответ на предъявленные в ходе процедуры стимулов. Обработка происходит с помощью специальной компьютерной программы. Суть метода заключается в выявление латентных акустических характеристик голоса, которые обусловлены стрессовой реакцией организма. В основе этого механизма находятся результаты исследований физиолога Липпольда, который установил, что в состоянии полного расслабления и покоя скелетные мышцы испытывают миографический тремор (микровибрацию). В состоянии психофизиологического возбуждения этот тремор ослабевает или исчезает совсем [3]. Однако, как отмечается в ряде исследований, данный метод является низкоэффективным. Так американский специалист П. Экман в своей книге рассказывает о «машинах», способных якобы с высокой точностью определять ложь по голосу. Однако в работе акцентируется внимание на недостаточной обоснованности соотношения лжи и стресса. В инструкциях к этим приборам есть предупреждение пользователей о рисках пропуска лжецов, не испытывающих отрицательных эмоций, и, наоборот – «неправильно истолковать поведение правдивых людей, которые чем-то расстроены» [4].

Как отмечают С. И. Оглоблин и А. Ю. Молчанов, сама процедура обнаружения ложных сведений с опорой на голосовой анализатор стресса принципиально не отличается от процедуры классической детекции с использованием полиграфных устройств [5]. Авторы, обосновывая низкую достоверность результатов такого обследования, указывают, прежде всего, на использование недостаточного количества показателей одного канала. Это увеличивает субъективность результатов исследования, снижает их точность [5].

Ю.А. Холодный, рассматривая основные методы «криминалистической полиграфологии», указывает на акустический метод, реализуемый с помощью так называемых анализаторов стресса по голосу, ориентированного на диагностику идеальных следов события путем

оценки амплитудно-частотных характеристик голоса человека, а также психолингвистический метод, реализуемый в тех же целях путем контроля и оценки темпоральных (временных), лексических и синтаксических характеристик речи человека [6].

Разновидностью инструментальных средств выявления скрываемой информации является энцефалографический и магнито-энцефалографический методы исследования мозговой активности. В некоторых исследованиях приводятся убедительные данные об эффективности одного из данных методов. Так, в исследованиях способов повышения контроля работы операторов сложных промышленных систем и установок, а также в целях совершенствования проверки квалификации персонала при приеме на работу новых сотрудников применялся метод анализа энцефалограммы испытуемого. Изучение так называемой «вызванной активности» головного мозга на сложный визуально-когнитивный стимул в целях использования этого эффекта в целях выявления ложных сведений позволяет говорить о принципиально новых прогрессивных методах в этой области [7].

На протяжении ряда лет исследуются возможности разных альтернативных методов инструментальной диагностики ложных сведений. В некоторых статьях приводятся доводы в пользу возможной эффективности рассматриваемых альтернативных способов. Таким образом, все методы сводятся к группе направлений: анализ вызванных потенциалов мозга, изображений, полученных методом ядерного магнитного резонанса; измерение стресса в голосе; термография (измерение температуры участков тела); динамическое измерение диаметра зрачка глаза.

Интересным является метод термического анализа поверхности кожи. Разработаны специальные технические приборы, которые используются для оценки изменений кровоснабжения отдельных участков поверхности лица. Главной целью использования тепловизоров является обнаружение кратковременных изменений кровотока, обусловленных активностью симпатической нервной системы [9].

Также относительно новым направлением исследования выявления ложных сведений является измерение зрачковой реакции. Прежние визуальные наблюдения показали, что в процессе лжи действительно наблюдаются изменения размера зрачка [10]. В некоторых работах авторы отмечают, что, в частности, было показано, что зрачковая реакция возникает при ответах на все вопросы, относящиеся к преступлению, однако она более выражена при ложных ответах на них [10].

В ряде работ в качестве наиболее перспективного метода отмечается метод термоэнцефалоскопии (метод, анализирующий активность коры головного мозга посредством регистрации локальных изменений температур), разработанный в Институте высшей нервной деятельности и нейрофизиологии РАН и в Институте радиоэлектроники (И. А. Шевелев) в 80-х годах прошлого века [10].

Такое изобилие инструментальных технических средств обнаружения скрываемой информации позволяет комплексно подходить к проблеме оценки и верификации скрываемой информации в рамках противодействия преступлений в сфере высоких технологий, совершаемых с применением методов социальной инженерии.

Библиографический список

1. https://dic.academic.ru.
2. Брутян Г. Паралогизм, софизм и парадокс // Вопросы философии. – 1959. – № 1. – С. 56–66.
3. Пеленицын А. Б., Степанов А. А. Детекторы лжи по голосу [Электронный ресурс]: код доступа: http://poligraf.sp.ru.
4. Экман П. Психология лжи. Обмани меня, если сможешь. – СПб. : Питер, 2010. – 304 с.
5. Оглоблин С. И., Молчанов А. Ю. Инструментальная «детекция лжи». – Ярославль : Нюанс, 2004. – 417 с.
6. Холодный Ю. И. Криминалистическая полиграфология и ее применение в правоохранительной практике // Информационный бюллетень № 21 по материалам криминалистических чтений «Запросы практики – движущая сила развития криминалистики и судебной экспертизы». – М. : Академия управления МВД России, 2003. – С. 14-19.
7. Коршаков А. В., Шатерников В. Е. Идентификация и определение достоверности принятых решений по вызванной энцефалографической активности // Промышленные АСУ и контроллеры. – 2013. – № 8. – С. 20–25.
8. Дженнифер Вендемия Детекция лжи // «Polygraph». – 2003. – № 32 (2). – С. 97–106. – [Электронный ресурс]: код доступа: http://www. poligraftest.ru.
9. Навваро Д., Карлинс М. Я вижу, о чем вы думаете. – Минск : «Попурри», 2009. – 336 с.
10. Оглоблин С. И., Молчанов А. Ю. Инструментальная «детекция лжи». – Ярославль : Нюанс, 2004. – 417 с.

И. А. Виноградова [1]

ИСТОКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: ВЗГЛЯД С ПСИХОЛОГИЧЕСКОЙ ТОЧКИ ЗРЕНИЯ

Если рассматривать результаты общедоступной научной деятельности, то можно наблюдать, что социальная инженерия – это молодое направление. Оно зародилось приблизительно в середине прошлого столетия в Европе и США.

«В послевоенный период мотивы социальной инженерии стали широко применяться в авиационной и оборонной промышленности Америки, а также в прикладных научных областях: индустриальной социологии, военной социологии, исследованиях пропаганды и коммуникаций, групповой динамики. Так, до 1949 г. в США действовала лишь одна научная группа по «человеческой» и социальной инженерии, к середине 60-х годов их насчитывалось уже более 130, и в их составе трудилось более 1,5 тыс. специалистов. Большинству из них финансовую поддержку оказывало правительство. В настоящее время часть специалистов по социальной инженерии работает в сфере частного бизнеса. При университетах и колледжах США функционируют многочисленные курсы подготовки по социальной инженерии» [1].

В России развитие социальной инженерии наблюдается с 80-х годов XX в., однако нельзя совершенно точно утверждать, что ранее исследований не было: скорее они были недоступны большинству. «Социальное прогнозное проектирование, стратегическое планирование, социальная инноватика, игровое моделирование – вот лишь некоторые из названий, за которыми зачастую скрывалось содержание социоинженерной деятельности» [1]. Наиболее яркий интерес к социальной инженерии в нашей стране стал проявляться с 90-х годов. Тогда научные сотрудники О. А. Уржа, Ю. М. Резник, В. В. Щербина и их коллеги пытались создать отечественное социоинженерное направление, но не получили поддержку от государства. Однако позже эта область вновь стала набирать обороты в нашей стране, что продолжается по сей день.

К сожалению, современная литература по социальной инженерии преимущественно носит лишь публицистический характер, и пестрит историями о людях, что «обошли систему». В целом человек, который ловко орудует социоинженерными методами, позиционируется как

---

[1] Студент 2 курса Московского педагогического государственного университета. © Виноградова И. А., 2018.

находчивый, с высоким адаптационным потенциалом, и это, конечно, является хорошими качествами, но граница между приспособлением к ситуации и вредительством ныне очерчена неявно.

Социальная инженерия оказалась разносторонним понятием, которое исследуют в контексте истории, политики, социологии и психологии. Но надо сказать, в первую очередь социальная инженерия в годы своего становления рассматривалась применительно к государственному управлению.

Наиболее распространенным определением социальной инженерии (в контексте социологии) является следующее: социальная инженерия – это совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним.

Так, например, одно из первых упоминаний социальной инженерии появилось в научных работах австрийского социолога и философа – Карла Поппера. Одну из основных работ – «Открытое общество и его враги» – К. Поппер смог опубликовать только в 1945 г., в Лондоне, спустя несколько лет после ее написания. В этой работе он, затрагивая феномен социальной инженерии, описывал концепцию «открытого общества». Согласно концепции этот термин означает общество, открытое неизвестному будущему, готовое к трансформации своих структур с применением рационального подхода и демократических институтов (их наличие подразумевало отсутствие насилия при внедрении этих изменений). Ценности такого общества схожи с либеральными: свобода для каждого человека, индивидуализм, возможность рационального управления государством. Основная проблема, которую пытается решить К. Поппер принцип управления обществом, государством, при условии сохранения его основополагающих ценностей.

В своей работе он выделяет два подхода: историцизм и социальная инженерия.

Суть историцизма заключается в вере в историческую предопределенность, в то, что существуют тенденции и законы, согласно которым развивается государство. Это значит, что развитие можно предсказать с учетом знания и понимания принципа работы этих законов.

Суть же социальной инженерии в гибкости, приспособляемости к окружающим динамичным обстоятельствам с тем, чтобы достичь поставленной цели. Она рассматривает институты как средства, обслу-

живающие определенные цели, и оценивает уровень их организованности с точки зрения их целесообразности, эффективности и простоты. Таково описание австрийского социолога.

Позволю себе немного перефразировать задачу социальной инженерии. В более общем виде она звучит так: каким образом можно использовать/трансформировать все имеющиеся ресурсы для достижения поставленной цели так, чтобы совершенные действия не стали разрушительны или ощутимы для окружающей системы. И хоть изначальная, теоретическая и в некотором плане утопическая цель была использование этого подхода во благо, мы четко понимаем (и видим этому подтверждения), что такой подход наделен и второй «стороной медали»: особенно ярко это можно наблюдать в сегодняшние дни, потому как за этим понятием все увереннее закрепляется преступный характер. Социальная инженерия стала крайне распространена среди мошенников, цель которых – получение выгоды в разнообразных ее проявлениях, и средства здесь эту цель всегда оправдывают. Злоумышленники стремятся повлиять на своих жертв, втереться в доверие так, чтобы получить нечто, что представляет собой ценность (информация, услуга, деньги). Одновременно с этим жертва, ничего не подозревая, предоставляет это «нечто» добровольно, без сопротивления, а значит, законно.

Причина этому очевидная и не новая: человек легко поддается внешнему воздействию, и не зря является наиболее слабым звеном в системе по сравнению с машинами, ведь на него можно найти рычаг давления (семья, амбиции, деньги и т. п.). И для понимания принципа воздействия на людей, предлагаю рассмотреть социальную инженерию с точки зрения психического процесса личности.

Мы знаем, что психика человека, если говорить в общем, имеет две составляющие – сознательную и бессознательную. Поскольку чаще всего человек не осознает влияние на себя со стороны мошенника, мы можем сделать вывод, что это влияние направлено на его бессознательную часть. Язык бессознательного – это эмоция, она первична. Но следует учесть, что эмоция всегда идет в привязке с образом. Так, какой-либо образ может легко вызвать эмоцию, которая ассоциируется у нас с ним (например, если мы увидим на улице человека с ножом, мы испытаем страх).

Личность человека комплексна. Она включает в себя огромное количество таких пар «эмоция+образ», однако мы можем их поделить на три группы: положительно-эмоциональные, отрицательно-

эмоциональные и нейтрально-эмоциональные образы. Это то, чем мы наполняем себя с приобретенным опытом и знаниями, так называемое информационное наполнение личности, которое явным образом влияет на качество мышления человека, даже можно сказать формирует его.

И все эти пары равны между собой до тех пор, пока не появляется доминирующая эмоция. Она оказывает влияние на остальные связки «образ + эмоция», а значит, и на мыслительный процесс в целом. Таким образом, деятельность нашего мышления осуществляется под влиянием эмоционального фона, сформированного этой доминирующей эмоцией. Происходит реструктуризация связей предметов и явлений действительности в сознательной и бессознательной сфере личности. Например, человек очень любит природу. Наблюдать ее пейзажи – большое удовольствие для него, которое воздействует положительно. А вот высоты боится. Представим, что он оказывается на большой высоте вокруг природных пейзажей (например, полетел на парашюте, привязанном к катеру тросом). В этом случае страх высоты станет доминирующим и не позволит полностью насладиться окружающим видом, а сосредоточит мысли человека на том, чтобы скорее вернуться с воздуха на землю. Получается, что эмоциональный фон, созданный одной эмоцией (негативной), перекроет вторую (положительную).

К сожалению или к счастью, мы не можем видеть эмоции других, а можем только по внешним признакам предположить, что испытывает человек. Однако, на появление эмоционального фона можно повлиять действиями извне. Это происходит потому, что эмоция по своей сути заразительна. Например, если мы слушаем прекрасного докладчика на конференции, мы перенимаем его настрой, у нас останется положительно-эмоциональный образ от его доклада. И позже, когда мы будем восстанавливать в памяти это мероприятие, мы по образу докладчика воспроизведем эмоции, которыми он нас «заразил».

Все это означает то, что возможно спровоцировать появление нужного эмоционального фона у человека и инициировать с помощью этого выполнения требуемого действия. Это идея, вокруг которой построены принципы социальной инженерии сегодня.

С появлением Интернета, альтернативных каналов живого общения эта идея осуществляется проще. Применяя социальную инженерию на различных интернет-сервисах (сайты с объявлениями, интернет-банки, интернет-магазины, лотереи в глобальной сети, сайты знакомств, консалтинговые услуги, электронная почта), в социальных сетях, мес-

сенджерах, при использовании мобильной связи, мошенники получают бонус: все эти каналы подразумевают обезличенность злоумышленника, делают его «невидимкой», потому в значительной мере усложняют процесс его идентификации и поимки (к тому же, правовое регулирование этого вопроса на данный момент приспосабливается к ситуации медленнее, чем происходит развитие мошеннических схем). Помимо этого злоумышленники активно пользуются неосведомленностью граждан о том, какие данные о себе можно сообщать сторонним лицам, а какие нет; какие последствия может повлечь за собой размещение данных о себе в социальных сетях и пр.

Все это указывает на то, что невозможно избежать социоинженерных атак в целом, но возможно повысить уровень осведомленности человека не только в части используемых злоумышленниками методов социальной инженерии, но и в части психологической безопасности или стойкости личности к внешним воздействиям на психику.

В заключение хотелось бы сформулировать вопросы, которые являются, на мой взгляд, наиболее острыми сегодня:

Определение границы между применением социальной инженерии во благо и во вред. Внедрение в массы осознания этой границы.

Стремительное повышение осведомленности общества о принципе работы социальной инженерии и о ее практических проявления.

Повышение уровня психологической устойчивости общества к воздействиям извне на психику.

Библиографический список

1. Дунаев В. Ю., Курганская В.Д . Социоинженерные технологии в управлении трансформациями казахстанского социума: монография / под общ. ред. З. К. Шаукеновой. – 2013. – URL: http://iph.kz/doc/ru/548.pdf.

И. В. Ульянова [1]

ПРОСВЕТИТЕЛЬСКАЯ РАБОТА ИНСПЕКТОРА ПДН С НЕСОВЕРШЕННОЛЕТНИМИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ ПО ПРЕДУПРЕЖДЕНИЮ КИБЕРМАНИПУЛИРОВАНИЯ ЛИЧНОСТЬЮ В СОЦИАЛЬНЫХ СЕТЯХ

Постиндустриальное общество, в формате которого в настоящее время развивается и Россия, характеризуется не только как потребительское, сервисное, но и как информационное. Информационность как социокультурную характеристику необходимо рассматривать дуально, раскрывая сущность позитивных и негативных влияний на развитие человека.

Например, Д. Белл подчеркивал в свое время ценность гуманитаризации, интенсивной информатизации человека нового этапа развития цивилизации. Тогда как Г. Маркузе и др. в своих трудах раскрыли антигуманистические тенденции информатизма, подчеркивая, что большой объем информации делает ее все «менее и менее полной», обостряет проблему восприятия информации отдельно взятым человеком. Более того, в связи с масштабным разнообразием подачи информации, ее навязчивостью, наличием потребительского подтекста, а также фрагментарностью, морально-нравственной неопределенностью, парадоксальностью человеку все сложнее противостоять эмоциональным перегрузкам, укреплять свою личностную уникальность и самостоятельность [6].

Киберсреда – виртуальная реальность (ВР, англ. – virtual reality, VR, искусственная реальность) – созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие. Для создания убедительного комплекса ощущений реальности компьютерный синтез свойств и реакций виртуальной реальности производится в реальном времени. Генеральный директор «Лаборатории Касперского» Е. В. Касперский подчеркивает: мир входит «в эпоху кибертерроризма. Мы пережили недавно три шока: терроризм, финансовый кризис и политический кризис. Следующий мировой шок – кибертерроризм и кибератаки. Мы

---

[1] Профессор кафедры педагогики МосУ МВД России имени В.Я. Кикотя доктор педагогический наук, профессор. © Ульянова И. В., 2018.

зависим от компьютерных систем, и нет ни одной полностью защищенной страны» [3].

Таким образом, сегодня выявляется новая форма управления человечеством, отличающаяся крайне слабым контролем, размыванием педагогических основ в процессе гуманистического воспитания подрастающего поколения. Одна из самых ярких черт выявляемого антипедагогизма – недифференцированность информации (если классификационным основанием являются морально-нравственная основа развития личности, аксиологический дискурс). Посредством интернет-системы, вход в которую осуществляется через компьютеры, айфоны (их продажа стимулируется специальной индустриальной отраслью), дети и подростки планомерно превращаются в первоочередных потребителей медиа техники и продукции в целом.

Социальные сети – в совокупности платформа, онлайн-сервис и веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете. Несмотря на кажущуюся изначально нейтральность социальных сетей (Facebook, Instagram, Twitter (США), В Контакте, Одноклассники (Россия) и др., она представляют собой открытые пространства для рекламы, целенаправленных воздействий и проч. Опрос, проведенный на портале Государственного университета ВШЭ, показал, что (по мнению респондентов) сети «затягивают» и отнимают слишком много времени, вытесняют реальное общение, обеспечивают «избыточность общения и информации». Тогда как вопросы конфиденциальности беспокоят пользователей социальных сетей в меньшей степени, преимущественно эти страхи связаны с легкой доступностью контактной информации для спамеров, а не с работой спецслужб. В подобных условиях развиваются компьютерная, сетевая аддикции, которые Всемирная организация здравоохранения с 2018 г. отнесла к болезням.

Еще одна из ярких черт данной кибер (информационной) среды с педагогической точки зрения – это ее слабая контролируемость на предмет соблюдения моральных норм и законодательства. Если законопослушные взрослые субъекты, в силу психологической зрелости в определенной мере способны регулировать процесс пребывания в социальных сетях (регламентировать время пребывания, оценивание содержания постов и проч.), то несовершеннолетние в объективном оценивании проблемной ситуации беспомощны, ведут себя наивно, доверчиво, что обусловлено возрастными особенностями, недостаточной критичностью, незрелостью морально-нравственной сферы, саморегу-

ляции. В связи с этим детско-подростковая среда является наиболее благоприятной для вовлечения несовершеннолетних в социальные сети с дальнейшим их киберманипулированием (примером служат сообщества «Синий кит», «Киберготы» и прочие).

С психолого-педагогической точки зрения манипулирование трактуется в научной литературе как «воздействие на кого-либо в целях возбуждения у него намерений, не совпадающих с его реально существующими желаниями, целями». Таким образом, выявляется абсолютно антигуманистический характер влияния на несовершеннолетних в киберсреде, когда отсутствует подлинная забота о развитии человеческой сущности ребенка, подростка, актуализируются сциентистско-автократический, бихевиоральный подходы к организации взаимодействия подрастающего поколения со старшим поколением.

В данных условиях сотрудник подразделения по делам несовершеннолетних органов внутренних дел (ПДН ОВД) оказывается в крайне сложной ситуации. В частности, принятая в 1989 г. Конвенция о правах ребенка (ООН) в настоящее время обладает положениями, которые вступают в противоречие с теми киберрисками, в которые вовлекается несовершеннолетний. Например, в статье 6 говорится об обязанности государства «обеспечивать его психическое, эмоциональное,<…> социальное, культурное» здоровье, а в статье 16 о Защите права на личную жизнь говорится о том, что право на личную жизнь ребенка связано с недопустимостью «читать его письма без разрешения». Тогда как компетентному специалисту в области детства понятно, что без реального контроля за контактами несовершеннолетнего в социальных сетях, изначально нацеленных на манипуляцию участниками группы, невозможно оказание полноценной и своевременной помощи. Столь же противоречивой представляется сейчас и статья 17, текст которой гласит: «Каждый ребенок имеет право на доступ к информации. Государство должно поощрять средства массовой информации к распространению материалов, которые способствуют духовному и культурному развитию детей, и запрещать доступ к информации, наносящей вред ребенку». Возникает вопрос: каким образом должен и может осуществляться данный запрет?

Очевидно, что социально-педагогическая работа по профилактике киберманипулирования личностью в социальных сетях крайне затруднена в связи с недосягаемостью непосредственных руководителей, гипердинамичностью всей киберсистемы. Вместе с тем, очевидна и стагнация деятельности компетентных органов, отвечающих за безо-

пасность детей и подростков в киберпространстве: например, Концепция информационной безопасности детей (утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р) не функционирует в формате федеральной программы. Вынужденно декларативным остается и предложение В. А. Плешакова – ведущего специалиста в сфере киберсоциализации – по поводу введения в школьную программу учебной дисциплины «Киберэтикет» и проч.

Таким образом, в современных реалиях комплексная работа по снижению опасностей в пространстве Интернета, социальных сетях в настоящий период будет эффективной, реальной в случае ее реализации в локальных условиях, в рамках конкретной образовательной организации. Она должна опираться на принципы системности, гуманности, а также деятельностный, личностно-ориентированный, средовой, смысложизненноориентационный подходы (Ю. С. Мануйлов, В. А. Сластнин, В. А. Сухомлинский, И. В. Ульянова и др.).

Реализация принципа системности предполагает устойчивое взаимодействие всех институтов, связанных с воспитанием подрастающего поколения: семьи, образовательных организаций, учреждений дополнительного образования, подразделений по делам несовершеннолетних; принцип гуманности ориентирует всех субъектов, реализующих позицию воспитателя, на заботу о подопечном, уважение к нему и эффективное содействие в его социализации, инкультурации. Обращение к вышеперечисленным подходам указывает на необходимость вовлечения несовершеннолетних в продуктивную деятельность с учетом их возраста, интересов, способностей (которую педагоги, родители не только отслеживают, фиксируют, но и стимулируют, направляют, корректируют); учет индивидуальных особенностей ребенка, подростка, их гендерную специфику, социокультурный статус; обеспечение комфортной среды, актуальных средовых ниш; на важность содействия личности в интериоризации гуманистических ценностей, постановке ближних и дальних целей, включения в актуальные виды деятельности, что присуще педагогике смысложизненных ориентаций.

Основой реализации таких действий должна служить воспитательная система школы – уникальный педагогический феномен, обеспечивающий «взаимодействие основных компонентов воспитания (целей, субъектов, их деятельности, общения, отношений, материальной базы) и обладающий такими интегративными характеристиками, как образ

жизни коллектива, его психологический климат» (Л. И. Новикова и др.).

В частности, в условиях воспитательной системы формирования смысложизненных ориентаций школьников (И. В. Ульянова) важным направлением деятельности педагогического коллектива является профилактическое. Оно ориентировано на три уровня реализации: первичная профилактика (ориентирована на предупреждение неблагоприятного воздействия на человека факторов социальной и природной среды), вторичная профилактика (направлена на предотвращение возможных нарушений моральной регуляции при первичном проявлении поведенческих нарушений), третичная профилактика (как совокупность мероприятий, направленных на коррекцию поведения, ее переориентацию, а также реабилитацию).

Субъекты, реализующие профилактическое направление, с учетом интенсивности взаимодействия с обучающимися условно разделены на два уровня: первичный и вторичный (что нисколько не снижает значимость специалистов «второго эшелона», но позволяет более четко определить их полномочия). Очевидно, что учителя, классные руководители, педагоги-психологи, социальные педагоги, систематически взаимодействуя с подопечными, сотрудничая с их семьями, более глубоко, тонко проникают в сущность возможных и реальных девиаций обучающихся (важным элементом их деятельности является ведение социально-психолого-педагогических карт классов, ориентация на указанные три уровня профилактической работы. В то же время специалисты вторичного уровня, куда входят инспектор ПДН, представители наркодиспансера, сотрудники социально-реабилитационных центров, преподаватели гуманитарных вузов и другие социальные партнеры образовательной организации, систематически и планомерно взаимодействуют со школьниками, педагогами, родителями, представителями смежных служб и организаций.

В системе профилактической работы весьма значимой является просветительская работа инспектора ПДН ОВД с несовершеннолетними в образовательных организациях (именно на их территории!) по предупреждению киберманипулирования личностью в социальных сетях, которая структурно выглядит следующим образом:

Социальный заказ семьи, общества: обеспечение безопасного пребывания несовершеннолетнего в киберсреде и снижение правонарушений и преступности несовершеннолетних в условиях киберсреды и на основе взаимодействия с ней (как следствия).

Цель: организация просветительско-профилактической эффективной деятельности с образовательными организациями, семьями, несовершеннолетними.

Субъекты взаимодействия: администрация образовательной организации, педагогический коллектив, социально-педагогическая служба, обучающиеся и их родители.

Формы взаимодействия: массовые (педагоги, родители), групповые (обучающиеся).

Виды сотрудничества: лекция с элементами беседы (педагоги и родители), беседа с учетом возраста в условиях классного часа «Правовое воспитание» (1-11 классы), совместные просветительско-профилактические проекты «Безопасная киберсреда школьника».

Концептуальные положения мероприятий:

1. Ориентация на Законы Российской Федерации и подзаконные акты, связанные с вопросами кибербезопасности несовершеннолетних и профилактика подростковых правонарушений в киберсреде. Учет законодательных противоречий.

2. Сотрудник ПДН ОВД – полицейский с педагогическим образованием, обладающий компетенциями в области защиты прав ребенка, его жизненной среды, в том числе информационной. Права и обязанности семьи, педагогического сообщества.

3. Сотрудничество социальных институтов как актуальный ресурс эффективной деятельности сотрудника ПДН ОВД.

4. Владение сотрудником ПДН ОВД объективной информацией о сущности предупреждения киберманипулирования личностью несовершеннолетнего (школьника) в социальных сетях.

5. Просвещение сотрудником ПДН ОВД субъектов образовательного пространства по проблеме: несовершеннолетний (школьник) как участник социальных сетей (сущность, риски и опасности).

6. Просвещение сотрудником ПДН ОВД субъектов образовательного пространства по проблеме: несовершеннолетний (школьник) как манипулятор и/или жертва киберманипулирования в социальных сетях.

Библиографический список

1. Ефимов Е. Г. Социальные Интернет-сети (методология и практика исследования). – Волгоград : Волгоградское научное издательство, 2015. – 168 с.

2. Калинина Т. В., Ручкина А. А. Компьютерная зависимость у детей подросткового возраста // Молодой ученый. – 2016. – № 21. –

С. 822–824. – Интернет-источник: URL: https://moluch.ru/archive/125/34491/ (дата обращения: 28.01.2018).

3. Касперский Е.В. Мир перед угрозой. – Интернет-источник: URL: https://info.sibnet.ru›article/280529 (дата обращения: 28.01.2018).

4. Концепция информационной безопасности детей (утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р). – Интернет-источник: URL: https://fk-karg.edusite.ru (дата обращения: 03.02.2018).

5. Краснова С. В. и др. Как справиться с компьютерной зависимостью. – М., 2013. – Интернет-источник: URL: https://twirpx.com/file/350392 (дата обращения: 20.01.2018).

6. Маркузе Г. Одномерный человек: исследование идеологии развитого индустриального общества / пер. с англ., послесл., примеч. А. А. Юдина; сост. и предисл. В. Ю. Кузнецова. – М. : ООО «Издательство АСТ», 2002. – 526 с.

7. Никитина Е. О. Внедрение современных информационных технологий в системе МВД России // Наука и школа. – 2012. – № 3. – С. 34–36.

8. Прокурова С. В. Компьютерная и игровая зависимость и профилактическая деятельность по ее преодолению // Современные проблемы науки и образования. – 2015. – № 2-2. – URL: https://science-education.ru/ru/article/view?id=23201 (дата обращения: 28.01.2018).

9. Юсов А. Б. Критика теории постиндустриального общества // Проблемы современной экономики. – 2011. – № 1. – С. 36–38.

В. И. Алескеров [1]

НЕКОТОРЫЕ СПОСОБЫ ВЫЯВЛЕНИЯ ЛИЦ, СОВЕРШАЮЩИХ КИБЕРПРЕСТУПЛЕНИЯ

В настоящее время лица, совершающие различного рода преступления, зачастую прибегают к возможностям сферы телекоммуникаций и компьютерной информации. Так, если в недалеком прошлом они использовали простые методы их совершения, то на сегодняшний день с учетом быстро развивающейся всемирной глобальной сети «Интернет» [2] такие лица хорошо осведомлены о современных возможностях информационных технологий, которые широко их используют для достижения своих преступных корыстных целей. Данный вид преступлений в обществе относят к киберпреступности [1] (совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках компьютерных систем или сетей, также против компьютерных систем, компьютерных сетей и компьютерных данных). Если взять для примера и рассмотреть часто совершаемый вид преступлений, как незаконное распространение наркотических средств и сильнодействующих психотропных препаратов, то вырисовывается такая парадоксальная линия, которая заключается в следующем.

В большинстве случаях преступники, являющиеся как организаторами, так и непосредственными распространителями в механизме преступлений, используют возможности современных телекоммуникационных технологий, а именно при незаконной реализации наркотиков, как устоявшееся правило, физически между собой не контактируют. Все их общение как на стадии договоренности, так и при незаконном получении наркотических средств, происходит с использованием мессенджеров (таких как: Telegram, WhatsApp, Viber, Imo)[2], шифрованных протоколов передачи данных и сеть «TOR»[3] (гибридная анонимная сеть, предоставляющая возможность передавать данные в зашифрованном виде, разработчиками которой является иностранная компа-

---

[1] Кандидат юридических наук, доцент, профессор кафедры ОТМ ОВД ВИПК МВД России. © Алескеров В. И., 2018.

[2] Telegram, WhatsApp, Viber, Imo – приложения для мгновенного обмена сообщениями в реальном времени через Интернет.

[3] TOR – гибридная анонимная сеть, предоставляющая возможность передавать данные в зашифрованном виде.

ния «Core Tor People» США, г. Сиэтл)[1]. За такой способ незаконного распространения оплата происходит по безналичному расчету с использованием электронных кошельков, банковских карт (путем перевода) и криптовалют[2]. Одной из самых популярных разновидностей криптовалют является биткойн (псевдоним разработчика Сатоси Накамото), который применяется для оплаты товаров и услуг. В частности, в сети «TOR» данная валюта применяется для оплаты различных незаконных сделок. Предметом данных незаконных сделок могут являться оружие, наркотики, торговля людьми и т. п. [3].

В качестве примера рассмотрим следующую информацию: наркодилеры отправляют крупную партию наркотиков, которая попадает на территорию Российской Федерации, и оптовые партии в дальнейшем распространяются по регионам. Далее товар фасуется по более мелким партиям и расходится по конкретным городам и регионам. После чего товар фасуется на более мелкие дозы по 0,5-1,5 грамма и раскладывается по тайникам-закладкам.

Рис. 1

Информация о закладке, а именно: координаты местности, фотография и описание тайника-закладки, передается непосредственному покупателю после осуществления им безналичной оплаты посредством электронных платежных систем [4].

---

[1] Core Tor People – компания-разработчик сети «TOR».

[2] Криптовалюта – разновидность цифровой (электронной) валюты, создание и контроль за которой базируется на криптографических методах (методы шифрования).

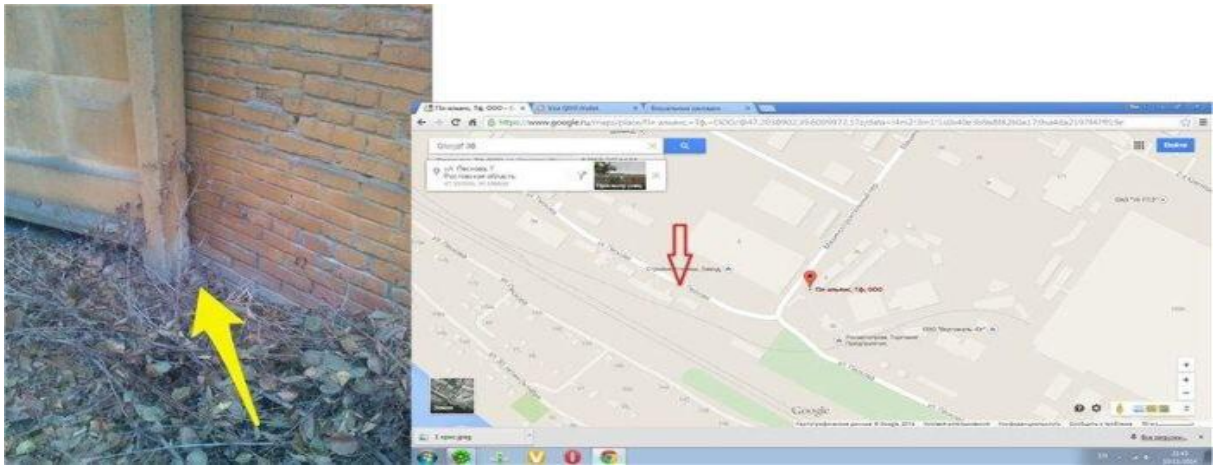


Рис. 2

В результате проведения комплекса оперативно-разыскных мероприятий, в том числе в сети «Интернет», устанавливаются лица, производящие тайники-закладки.

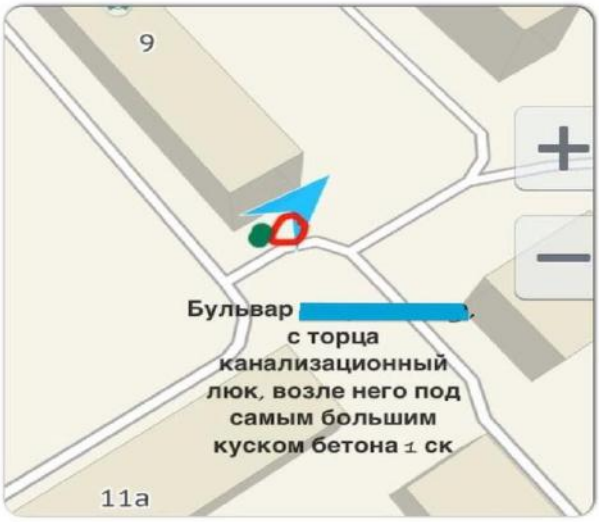


Рис. 3

Данные лица берутся под наблюдение [5] в целях последующего выявления администраторов данных ресурсов в телекоммуникационных сетях и оптовых распространителей наркотических средств. После осуществления соответствующих комплексных оперативно-разыскных мероприятий, проводимых в отношении лиц, попавших в поле зрения, их преступная деятельность документируется, выясняются все обстоятельства содеянного преступления, устанавливаются причастные к совершению преступления лица и, в конечном счете, они задерживаются.

Злоумышленники следят за активностью граждан у тех или иных банкоматов. Выбирают банкоматы с наибольшей проходимостью граждан, после чего определяют, оборудован ли банкомат и прилегающая к нему территория системой видеонаблюдения.

Рис. 4

Далее подбирают удобное время для установки скиммингового оборудования. На картридер[1] устанавливают устройство с магнитной головкой, замаскированное под рамку картоприемника, которое считывает информацию с магнитной полосы и записывает дампы карт на встроенную микросхему памяти.

Рис. 5

Кроме того, на клавиатуру банкомата устанавливается специальная и скрытая накладка, замаскированная под настоящую клавиатуру банкомата, которая при вводе ПИН-кода запоминает нажатия клавиш и также записывает их на встроенную микросхему.

[1] Картридер – устройство, предназначенное для считывания информации с банковской карты.

Рис. 6

Также устанавливается скрытая миниатюрная видеокамера, которая снимает систему набора цифр, составляющих ПИН-код[1], и записывает на встроенный модуль памяти либо передает видеосигнал дистанционно на оборудование злоумышленника.

Рис. 7

[1] ПИН-код – персональный идентификационный номер (аналог пароля).

Через некоторое время злоумышленник снимает скимминговое[1] оборудование с банкомата. В дальнейшем информация, полученная посредством указанного оборудования, синхронизируется по времени для последующего изготовления дубликатов банковских платежных пластиковых карт. После чего незаконно изготовленные дубликаты банковских карт передаются подельникам, которые в свою очередь обналичивают финансовые средства, находящиеся на банковских счетах потерпевших граждан, к которым привязаны банковские карты. Выявление и задержание лиц, осуществляющих данную противоправную деятельность, очень затруднительны. Устройства, предназначенные для негласного съема информации, практически неотличимы от оригинальных устройств банкомата и устанавливаются на короткий промежуток времени. При обнаружении факта установки скимминогового оборудования необходимо:

– в кротчайшие сроки организовать скрытое наблюдение за банкоматом и прилегающей территорией;

– дождаться и зафиксировать лицо или группу лиц, которые снимают данные устройства.

После задержания подозреваемых лиц с ними ведется работа, направленная на установление мест хранения и использования оборудования, предназначенного для незаконного изготовления поддельных банковских карт.

В настоящее время широкую популярность получили интернет-порталы, предназначенные для размещения объявлений о продаже товаров и предоставления услуг, с использованием которых злоумышленники совершают мошеннические действия. Наиболее распространенными видами мошеннических действий являются схемы, направленные на получение злоумышленниками денежных средств от пользователей данных ресурсов. Мошенник умышленно размещает объявление о продаже того или иного несуществующего товара с заведомо заниженной ценой в сравнении с рыночной. В ходе общения покупателя и мошенника посредством мобильной связи либо с использованием интернет-ресурсов[2] последний просит перевести денежные средства в качестве задатка за данный товар, ссылаясь на то, что имеется большой спрос на него. Покупатель, который по каким-либо причинам не может быстро добраться до места осмотра товара, переводит зло-

[1] Скимминг – кража данных банковской карты при помощи специального считывающего устройства.

[2] Интернет-ресурс – элемент сети «Интернет», например, веб-страница (сайт), почтовый сервер или поисковая система.

умышленнику деньги с использованием различных платежных систем. При этом денежные средства переводятся на счета мобильных телефонов, банковских карт, электронные кошельки и т. д. После чего злоумышленник обналичивает деньги и исчезает без предоставления товара либо услуги. Для установления лица, совершившего мошеннические действия, от оператора связи необходимо получить детализацию соединений абонента, установить, на кого зарегистрирован данный абонентский номер. Далее от администратора ресурса необходимо получить информацию об IP-адресе, с которого было размещено объявление, а в компании-провайдере запросить сведения об абоненте, которому в указанный период времени был выделен данный IP-адрес[1]. Кроме того, у представителей кредитно-финансовой организации необходимо получить информацию о движении денежных средств по счету, на который потерпевшим были переведены деньги, информацию о банкомате, с помощью чего были обналичены денежные средства с приложением видеозаписей, зафиксированных с камер видеонаблюдения. После установления данного лица проводится комплекс оперативно-разыскных мероприятий, направленных на его задержание.

В последнее время большой общественный резонанс вызвали факты доведения до самоубийства несовершеннолетних лиц посредством использования социальных сетей. В целях склонения к факту суицида использовались группы в социальной сети «Вконтакте», «Одноклассники» и др., в которых администратор группы предлагал ее несовершеннолетним участникам выполнить поэтапно последовательность заданий, представляемых в виде ролевой игры, последним этапом которой было совершение самоубийства. Особенностью своевременного выявления и последующего раскрытия подобных фактов является необходимость не только выявить администраторов групп, но и провести соответствующую профилактическую работу с участниками выявленных групп и предупредить случаи суицида. Во взаимодействии с администраторами социальных сетей осуществлялись выявление и локализация лиц-организаторов так называемых «групп смерти». В последующем во взаимодействии с провайдерами услуг доступа к телекоммуникационной сети устанавливались фактические места доступа в сеть «Интернет».

На 40-м заседании Национального антитеррористического комитета, которое прошло 11 июня 2013 г., директор ФСБ России Александр Бортников выступил с инициативой о необходимости разработки за-

[1] IP-адрес – уникальный сетевой адрес узла в компьютерной сети.

конопроекта, запрещающего использование сети «TOR» на территории Российской Федерации. Данную сеть используют члены незаконных бандформирований, действующих на территории Российской Федерации, и их сообщники для общения между собой, передачи информации и перевода денежных средств.

Рис.8

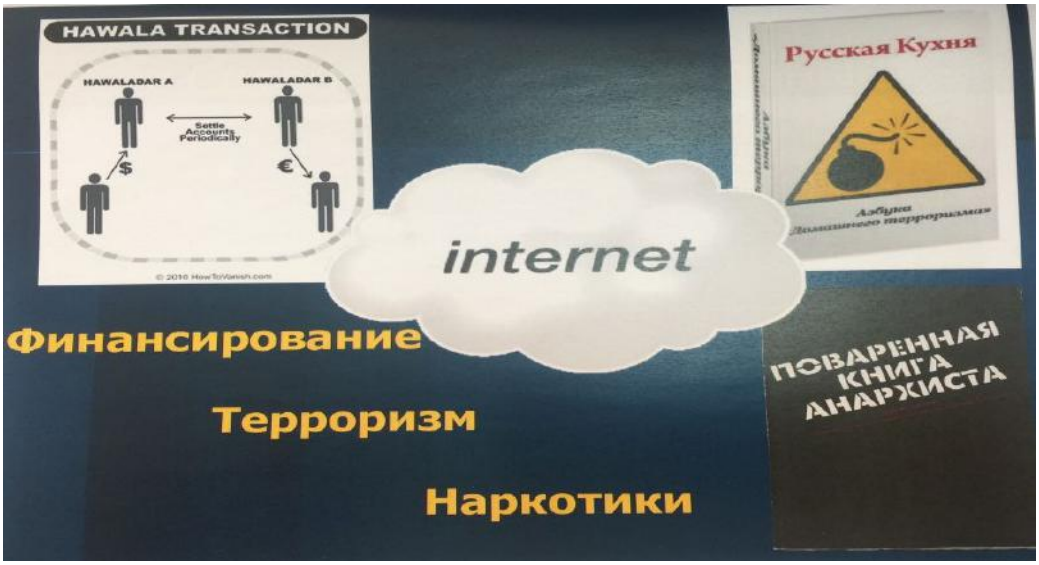


Рис. 9

Исходя из вышеизложенного, можно сделать следующий вывод, что установление лиц, осуществляющих противоправную деятельность в той или иной преступной среде с использованием сферы телекоммуникаций и компьютерной информации, а также их соучастников и лиц, оказывающих им всяческое содействие, а равно получение сведений о фактических пользователях закрытых сетей, на данный момент представляет собой огромную сложность для правоохранительных органов. В связи с этим необходимо исследовать возможность

получения технической информации о пользователях (пользовательском оборудовании) закрытых сетей, для чего необходимо повысить уровень профессиональных навыков у сотрудников оперативных служб и в ряде случаев следователей, а также улучшить материальную базу технико-криминалистическим обеспечением.

Библиографический список

1. Шамонини А. В., Баранов В. В. Организация выявления, раскрытия и расследование хищений денежных средств в системе ДБО : учебно-практическое пособие / под науч. ред. докт. юрид. наук, проф. А. В. Шамонина. – М. : Академия управления МВД России, 2014. – 312 с.
2. Тарасов А. М. Электронное правительство и информационная безопасность : учебное пособие. – СПб. : ГАЛАРТ, 2011. – 648 с.
3. Овчинский В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия. – М. : Норма, 2017. – 528 с.
4. Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. … канд. юрид. наук. – М., 2016.
5. Шумилов А. Ю. Оперативно-розыскная деятельность в схемах и определениях : учебное наглядное пособие. – 4-е изд., испр. и доп. – М. : Издательский дом Шумиловой И. И., 2008. – 96 с.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Сборник научных трудов
Всероссийского круглого стола
15 февраля 2018 г.

НАУЧНОЕ ЭЛЕКТРОННОЕ ИЗДАНИЕ

В авторской редакции
Корректоры *Степанова А. А., Титова В. П.*
Компьютерная верстка *Татариновой О. А.*

Усл.-печ. л. 23,50.

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12