Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННЫХ СФЕРАХ

Всероссийская научно-практическая конференция
(26 ноября 2021 г.)

Сборник научных статей

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя
2021

ISBN 978-5-9694-1065-7

УДК 004.056
ББК 16.8
П83

Рецензенты:
начальник кафедры информационно-компьютерных технологий
в деятельности органов внутренних дел Белгородского юридического института
МВД России имени И. Д. Путилина кандидат технических наук,
доцент **А. Н. Прокопенко**; следователь по особо важным делам 1 отдела
(зонального контроля) управления ведомственного и процессуального контроля
Следственного департамента МВД России **И. М. Горбатых**

Составитель *И. С. Мельцева*

П 83 **Противодействие терроризму и экстремизму в информационных сферах** : Всероссийская научно-практическая конференция : сборник научных статей / [сост. И. С. Мельцева]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2021. – 190 с. – 1 электронный оптический диск (CD-R). – Системные требования : CPU 1,5 ГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.

ISBN 978-5-9694-1065-7

В сборнике публикуются статьи участников Всероссийской конференции «Противодействие экстремизму и терроризму в информационных сферах», прошедшей в Московском университете МВД России имени В.Я. Кикотя 26 ноября 2020 г.

В статьях рассматриваются основные аспекты распространения экстремизма и терроризма по всему миру, их негативное влияние на внутригосударственные и международные процессы, характеризуется идеологическая основа экстремизма и терроризма и приводятся правовые пути борьбы с ними. В работах отражены проблемные вопросы и перспективные направления по борьбе с экстремизмом и терроризмом в условиях цифровизации общества. Статьи публикуются в авторской редакции.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб;
Windows XP SP3; 1 Гб свободного места на жестком диске

Издание подготовлено
с помощью программного обеспечения Microsoft Word

Редактор *Абилова Ф. А.*
Компьютерная верстка *Абилова Ф. А.*

Подписано к изданию 24.12.2021
Объем издания: 3,19 Мб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1065-7

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
https://мосу.мвд.рф, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Минаев В. А.[1],
профессор кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор

Федорович В. Ю.[2],
заместитель начальника по научной работе
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ МЕДИА

В современном обществе обострились экстремистские проявления, проникнув во все сферы жизни и приведя к образованию мощных угроз его различным социальным группам. Деструктивному воздействию особенно подвержены подростки и молодежь, предпочитающие традиционным средствам распространения информации (телевидение, радио, газеты, журналы) применение высокоскоростных мессенджеров и социальных сетей.

Среди современных методов, применяемых для решения задач противодействия распространению идеологии экстремизма, перспективны разработки в области компьютерного имитационного моделирования [1–4] и методы искусственного интеллекта [5–7].

Полученные на их основе результаты позволяют систематизировать особенности и закономерности проявлений экстремизма в социальных сетях. Как в динамическом аспекте – временные особенности «информационного заражения», так в территориальном – параметры сетевых информационных связей и узлов в различных регионах.

На основе методов искусственного интеллекта получены важные результаты при выявлении деструктивного контента экстремистской направленности в социальных мессенджерах и социальных сетях. А именно, пропаганда нацизма, антисемитизма, радикального ислама, суицидального поведения подростков и др. Точность распознавания деструктивного контента – не менее 91 % [8–10].

Среди основных практических результатов, полученных на основе моделирования противодействия экстремистским проявлениям в социальных медиа, выступают:

– методы выявления деструктивного контента в социальных медиа, содержащего экстремистскую информацию;

– модели управления противодействием в информационных сетях с учетом дестабилизирующих влияний со стороны криминалитета;

– методы добывания сведений о лидерах, структуре и ресурсах преступных группировок.

Решение указанных задач позволяет повысить эффективность проведения правоохранительными органами операций с целью дестабилизации и функционального разрушения экстремистских организаций.

При моделировании динамики распространения идеологии экстремизма в социальных медиа (далее – СМ) основная цель заключается в обеспечении и поддержании связей между людьми, даже когда они находятся далеко друг от друга. Наряду с данным положительным явлением, имеется и отрицательная сторона применения СМ – это распространение деструктивной манипулятивной информации.

По данным исследования Brand Analytics «Социальные сети в России: цифры и тренды» [11], более трети россиян, используя социальные сети, пишут хотя бы один пост в месяц, а все вместе – 1,3 млрд публичных сообщений (постов, репостов и комментариев). Наиболее популярными по размещению контента площадками стали: ВКонтакте, Instagram, Одноклассники, Facebook, Twitter, YouTube. В последние два года к ним добавились Telegram и TikTok.

Действующие платформы продолжают прирастать аудиторией, происходит активное появление новых участников. Использование современных средств информационного воздействия (далее – ИВ), к сожалению, нашло большой практический интерес у экстремистских организаций. Оно позволяет им без серьезных материальных затрат негативно влиять на определенную аудиторию, осуществлять акции, влекущие за собой громкий общественный резонанс.

Приведем статистические данные, дающие представление о подверженности социальных групп россиян различным путям осуществления негативных ИВ [12]. Результаты приведены в табл. 1.

Из анализа табл. 1 следует, что наибольшее опасение вызывает риск мошенничества и воздействие навязчивой рекламы. С этим чаще всего сталкиваются пенсионеры в силу определенной ограниченности общения, низких компетентностей в экономической и финансовой областях, подверженности телевизионным технологиям воздействия.

В социальных группах подростков и студентов указывается на высокий риск агрессии. Здесь ведущую роль отводят кибербуллингу. Он проявляется в умышленном агрессивном поведении в интернете или мобильных телефонных сетях. Особенностью поведения является его направленность на того, кто слабее, с целью унижения достоинства.

Таблица 1

Подверженность социальных групп различным ИВ (%)

	Социальные группы	Неэтичная и навязчивая реклама	Мошенничество	Порнография	Психологическое давление	Агрессия	Экстремизм
1	Подростки	36	62	23	63	77	58
2	Студенты	43	55	34	57	78	61
3	Пенсионеры с низким уровнем дохода	78	81	45	35	76	71
4	Домохозяйки	80	66	38	42	62	56
5	Работающие (с низким уровнем дохода)	72	74	40	38	58	46
6	Работающие (с неполным средним, средним, начальным и средним профессиональным образованием)	64	79	36	24	54	46
7	Безработные	56	68	34	32	60	52

Поэтому наиболее вероятные сценарии воздействия со стороны экстремистов связаны с детьми, подростками, молодежью. Именно данным социальным группам следует уделять наибольшее внимание при модельных исследованиях распространения агрессивных и опасных преступных проявлений.

Учитывая весьма высокую подверженность социальных групп населения, особо уязвимых в информационно-психологическом отношении, существует необходимость создания глобальной распределенной базы данных и информационно-аналитической системы (далее – ИАС) мониторинга агрессивного и особо опасного преступного поведения (прежде всего, экстремистского характера) в масштабах страны.

В основу высокотехнологичного противодействия распространению экстремистской идеологии должны быть положены новейшие теоретические и практические результаты в области системного моделирования и информационных технологий.

Особое внимание при организации противодействия распространению деструктивной информации, продуцируемой экстремистскими структурами, должно быть уделено исследованию процессов, которые связаны с сетевой организацией инфокоммуникаций в современном обществе.

Агентный, системно-динамический и дискретно-событийный подходы, реализованные в виде имитационных моделей, предоставляют огромные возможности для исследования распространения экстремистской идеологии в социальных сетях. При этом системно-динамический подход позволяет наибо-

лее качественно описывать их распространение и управление противоборством с их влиянием.

Аппаратно-программной платформой для реализации системно-динамических моделей ИВ и ИПД выступала современная система имитационного моделирования AnyLogic.

Приведем результаты имитационного эксперимента [13–15], где исследуется зависимость скорости распространения экстремистской идеологии пользователями сети от частоты асоциальных контактов (рис. 1).

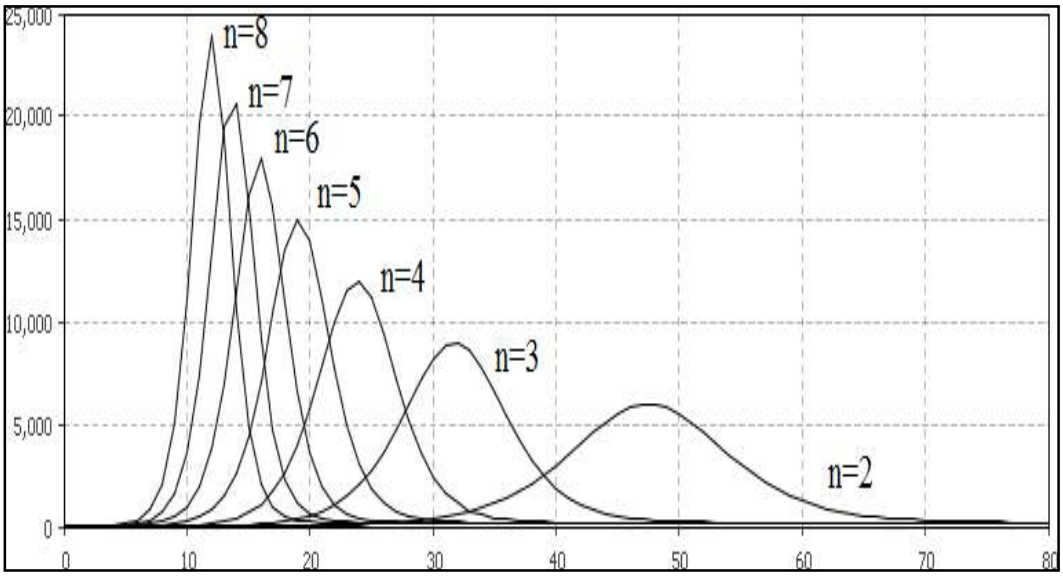


Рис. 1. Зависимость скорости принятия экстремистского воздействия от частоты асоциальных контактов

Из анализа рис. 1 следует, что, например, при двух контактах в день (n=2) скорость принятия экстремистской идеи достигнет своего максимума через 48 дней, а уже при восьми (n=8) – через 12 дней. Очевидно, что целенаправленное использование социальных медиа на порядки увеличивает указанные показатели, доводя их до нескольких часов. Подобную зависимость экстремистские структуры активно используют в своей вербовочной деятельности.

При моделировании эволюции экстремистских структур на основе подходов, предложенных в работе [16], в качестве антиэкстремистских мер рассмотрены две их категории, отражающие:

1. Жесткие стратегии борьбы (далее – ЖСБ). Они включают в себя нейтрализацию экстремистов радикальными методами вплоть до их физической ликвидации, тотальную проверку всех, продвигающихся через контрольно-пропускные пункты или блокпосты, и другие подобные меры. В целом данные действия влекут за собой существенные нарушения прав и значительный материальный ущерб непричастного к экстремизму населения. Вызывая тем самым недовольство и даже противодействие, в том числе – среди тех его групп, где экстремисты ищут и находят новых рекрутов. Таким образом, жесткие стратегии борьбы могут иметь прямую выгоду от ликвидации действующих

экстремистов, но и отрицательный косвенный эффект от стимулирования процесса вербовки новых членов экстремистских структур, используя для этого такой современный информационный инструмент, как СМ.

2. Интеллектуальные стратегии борьбы (далее – ИСБ). Это точечные, выверенные операции, в том числе – информационного характера. Они базируются на интеллектуальных решениях, направлены против лиц, виновность которых в экстремистской деятельности полностью доказана. Важная особенность подобных операций состоит в том, что они никак не затрагивают непричастное к экстремистской деятельности население.

ИСБ выглядят более приемлемой мерой в глазах населения и не подпитывают дополнительную вербовку в экстремистские структуры. Но такие стратегии дороже и сложнее в применении, чем ЖСБ. При проведении операций данного типа существует ряд ограничений, вызванных необходимостью высокой подготовки соответствующих кадров, в том числе – в области информационных технологий и информационной безопасности.

В рамках исследования эволюции экстремистской организации с учетом ее взаимодействии с населением региона, в том числе – через СМ, рассмотрены трехмерные модели [17, 18], учитывающие противодействие экстремизму со стороны правоохранительных структур.

Население региона рассмотрено в виде трех составляющих:

- экстремисты;
- восприимчивые как к экстремистской, так и к пацифистской пропаганде;
- невосприимчивые к такого рода информационным воздействиям.

Из анализа рис. 2 можно сделать вывод, что, используя информационное противодействие, в том числе и через СС, деструктивным влияниям экстремистского характера, можно оказать значительное влияние на пропагандистские возможности террористических групп.

Зависимость, изображенная на рис. 3, похожа на зеркальное отражение рис. 2. Но она отражает убыль численности экстремистов по квадратичному закону по мере роста антиэкстремистских мер.

Сравнивая зависимости на рис. 2 и 3, отметим, что для формирования эффективных мер борьбы в каждый момент времени важно понимать, какой процесс превалирует на данной территории – рост ЭП или его спад.

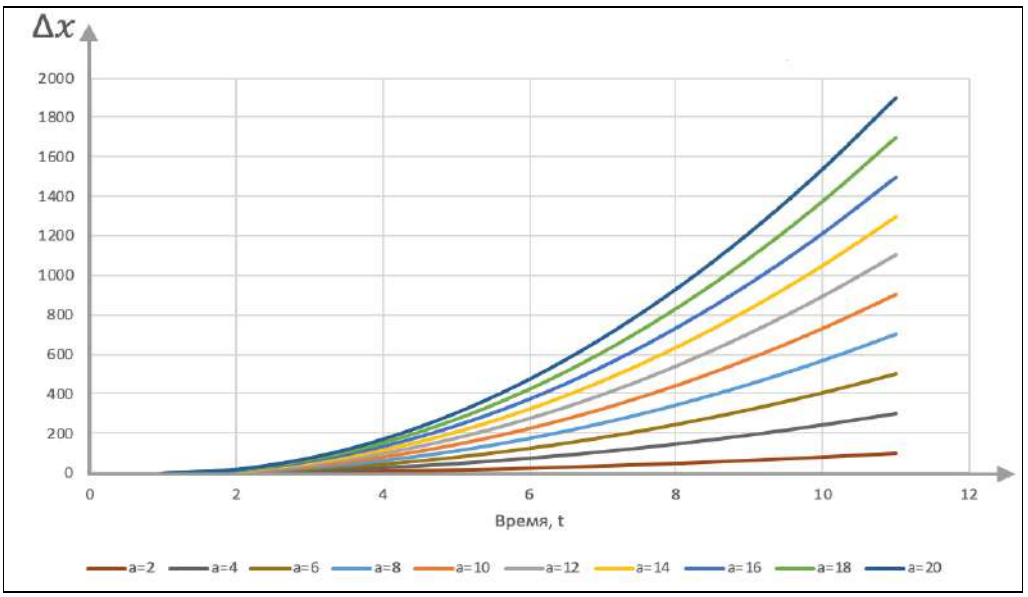


Рис. 2. Приращение численности террористов (Δx)
при увеличении эффективности вербовки (параметр a)

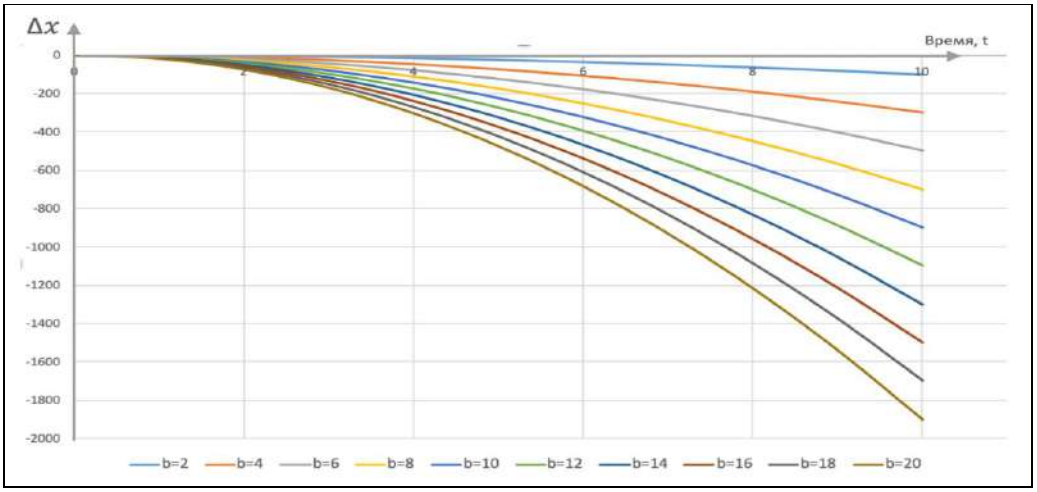


Рис. 3. Уменьшение размера экстремистской организации
с ростом мер противодействия экстремизму (параметр b)

Таким образом, принятие обоснованных и целенаправленных мер по борьбе с экстремизмом связано с системным пониманием и интерпретацией динамических изменений в структуре и характеристиках экстремистских организаций. Для этого в моделях целесообразно комплексно рассматривать как факторы воспроизводства экстремизма и борьбы с ним, в том числе, связанные с антиэкстремистской деятельностью со стороны правоохранительных органов, так и информационные взаимодействия различных региональных групп населения, в основном – в СМ.

В качестве результатов моделирования целесообразно комплексно рассматривать итоги реализации двух подходов: одномерного к воспроизведению особенностей эволюции размера экстремистской организации в зависимости от факторов ее внутреннего воспроизводства и деятельности антиэкстремистских

структур с различными стратегиями борьбы (жесткими и интеллектуальными), включая использование информационных возможностей СМ; и трехмерного, описывающего взаимосвязанные переходы между системой состояний, в которых может находиться региональное население, включая состояние «действующий экстремист». При этом переходы между состояниями определяются как информационными взаимодействиями между группами населения, относящегося к различным состояниям, так и деятельностью правоохранительных структур (в том числе – информационной) по борьбе с экстремизмом.

Моделирование территориальных различий распространения информации в социальных сетях

Для реализации модели территориальных различий распространения информации по специальной методике собраны статистические данные в социальной сети (далее – СС) в ВКонтакте по всем 647 населенным пунктам России с количеством жителей от 10 до 20 тысяч человек о топологии сети, ее пользователях, у которых выяснены все списки «друзей», зарегистрированных в этом населенном пункте. По группам «друзей» для всех населенных пунктов рассчитаны математическое ожидание, дисперсия, медиана, диаметр графа и средняя длина пути графа.

Для моделирования распространения информации в населенных пунктах использована указанная выше программная среда *Anylogic*.

В качестве характерных параметров, отражающих динамику распространения информации в региональных СС, как показали исследования, целесообразно выбрать время исхода 95 % индивидов из множества уязвимых к информационному воздействию, а также время достижения в популяции максимума индивидов в латентном состоянии («информационно заражен», но не распространяет деструктивную идею.

Как показали расчеты зависимостей указанных параметров применительно к статистическим характеристикам множества «друзей» в каждом из рассмотренных населенных пунктов, наилучшими (для объяснения) являются модели, зависящие от дисперсии, рассчитываемой по формуле:

$$D_i = \frac{1}{n_i} \cdot \sum_{j=1}^{j=n_i} (x_j - \bar{x}_i), \qquad (1)$$

где n_i – количество информационных узлов (пользователей) в *i*-м населенном пункте;
x_j – количество «друзей» у *j*-го пользователя в *i*-м населенном пункте;
$\bar{x}_i$ – среднее количество «друзей» в *i*-м населенном пункте; *i*=1, …, 647.

Исходя из того, что зависимость (1) достаточно хорошо объясняет территориальные особенности времени исхода 95 % индивидов из множества уязвимых целесообразно решить задачу выделения однородных групп населенных пунктов со схожими условиями распространения информации.

Такая задача успешно решена. Для выявления однородных групп среди всех исследованных 647 поселений Российской Федерации проведен их многомерный кластерный анализ. Для этого применительно к каждому поселению использовались конкретные статистические характеристики, отражающие *пользовательское сообщество,* и параметры *организации информационных сетей.*

В результате построены дендрограммы [13], позволившие выделить пять групп поселений, географически компактно и содержательно хорошо интерпретируемо расположенных на территории страны. Выявлены зависимости времени исхода 95 % индивидов из множества уязвимых к информационному воздействию (T_r), а также времени достижения в популяции максимума индивидов в латентном состоянии (T_k).

Как показано на рис. 3 и 4, соответствующие функциональные кривые (коэффициент объясняемости близок к 100 %) представляются соотношениями:

$$T_{rj} = 71.75 \cdot D_j^{-1.155} \quad (2)$$

$$T_{kj} = 56.9 \cdot D_j^{-1.153}, \ (j = 1, \ldots, 5) \quad (3)$$

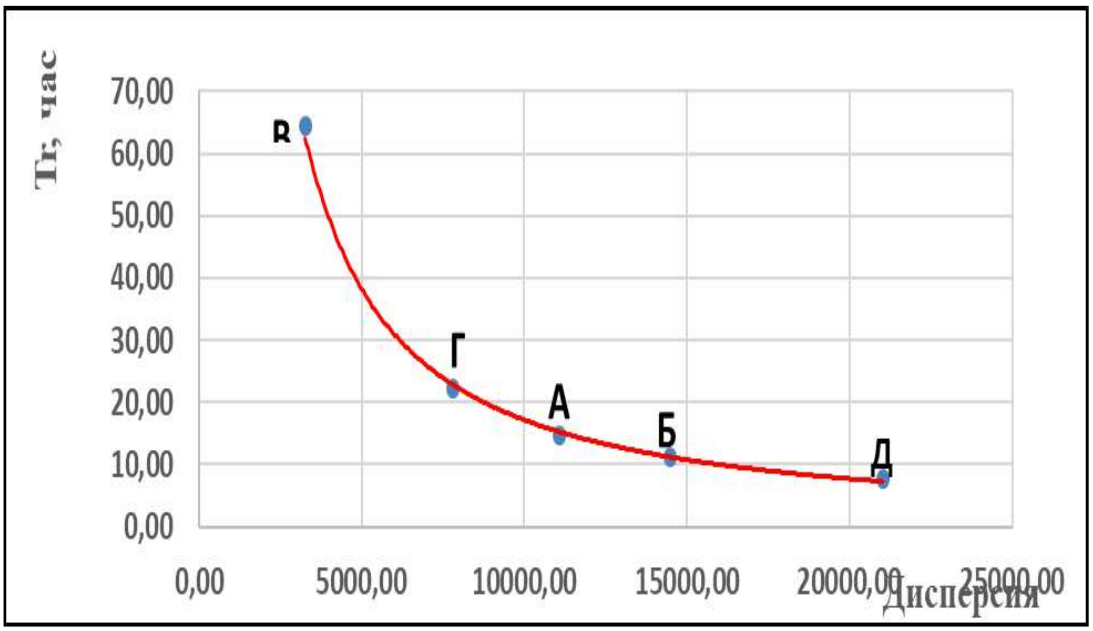


Рис. 4. Зависимость динамического параметра T_r от дисперсии (кружками обозначены эмпирические данные)

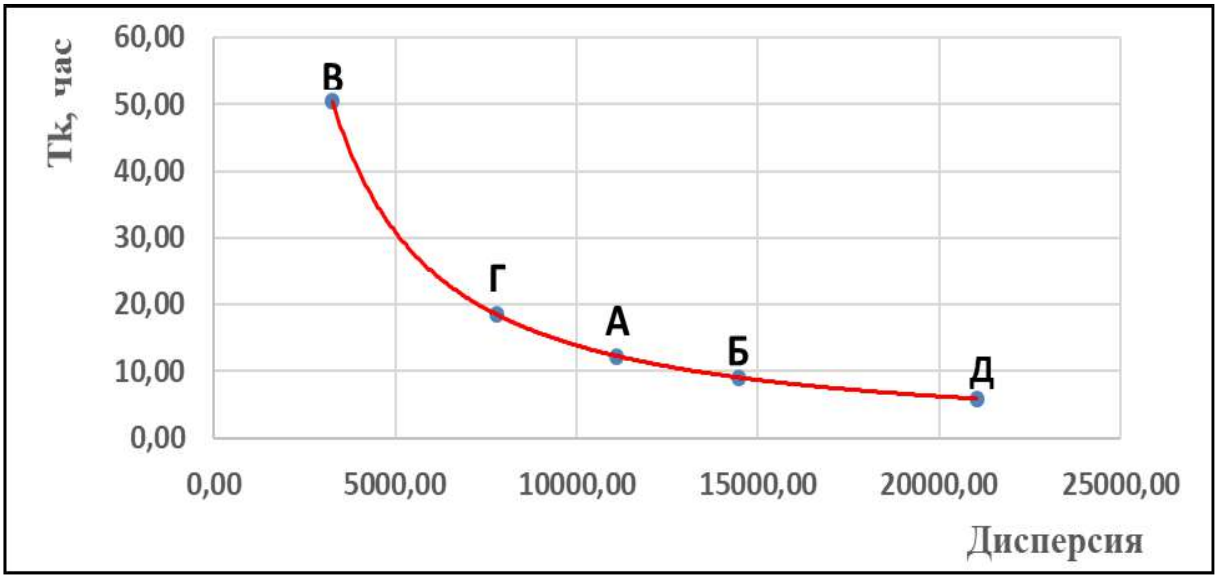


Рис. 5. Зависимость динамического параметра T_k от дисперсии (кружками обозначены эмпирические данные)

Итак, в процессе моделирования территориальных различий получены новые научно-практические результаты, важные для обоснования мероприятий противодействия распространению идеологии экстремизма в социальных медиа, а именно:

– найдено функциональное описание зависимостей времени исхода индивидов из состояния «уязвимые» к информационным воздействиям, а также времени достижения в популяции максимума индивидов в латентном состоянии, от дисперсии числа «друзей» пользователей СМ в однородной группе поселений кластеров;

– выявленные функциональные зависимости позволяет отделять одни поселения от других по степени восприимчивости населения к информационным воздействиям в СМ, включая деструктивные воздействия экстремистского характера. Последнее дает возможность органам власти, силовым структурам, образовательным организациям, исходя из принадлежности к тому или иному кластеру, целенаправленно строить политику и тактику противодействия таким влияниям;

– построено географически компактное территориальное распределение поселений кластеров, дающее возможность детально исследовать причины региональных различий скорости распространения информации, которые определяются как организацией сетевых сообществ и самих сетей на различных территориях, так и экономическими, социальными, демографическими, этническими и иными факторами проживающего там населения.

Методы выявления контента экстремистского содержания в социальных медиа

Приведем пример выявления контента экстремистского содержания в текстовых массивах из СМ: отражающих информацию антисемитского характера;

содержащих высказывания, направленные на реабилитацию нацизма; восхваляющих лозунги радикального ислама [8–10]. В табл. 2 приведены названия и объемы текстовых массивов в виде коротких сообщений из социальных мессенджеров и социальных сетей, исследованных на предмет экстремистского содержания, а также точность распознавания в процентах.

Таблица 2

Текстовые массивы, исследованные на предмет экстремистского содержания

Название текстового массива	Количество сообщений, тыс.	Точность распознавания, %
Антисемитизм	**268**	**91**
Реабилитация нацизма	**284**	**93**
Радикальный ислам	**310**	**95**

Из табл. 2 следует, что точность распознавания сообщений экстремистской направленности не менее 91 %, причем наилучшим образом выявляются тексты, содержащие различные формулировки из области радикального ислама – 95 %.

В статье показана необходимость глобального противодействия распространению идеологии экстремизма в социальных медиа, развития все более глубоких системных исследований факторов, определяющих тенденции этого опасного явления. Данное положение дел заставляет вырабатывать новые стратегии и тактики противоборства в этой сложной сфере и осуществлять дорогостоящие операции информационного характера со стороны государственных структур.

Указанные вопросы тесно связаны с планами МВД России в ближайшие годы в рамках национальной программы «Цифровая экономика Российской Федерации» создать крупный ведомственный Федеральный центр обработки данных (ФЦОД МВД России). Создание Центра обусловлено необходимостью обеспечения органов и подразделений МВД России высокопроизводительной и защищенной технологической инфраструктурой информационно-аналитического обеспечения, а также едиными информационными ресурсами.

Объединение информационных ресурсов на площадке ФЦОД позволит существенно модернизировать алгоритмы сбора, обработки и хранения данных, повысить качество решения задач по противодействию экстремизму, возложенных на МВД России, увеличить скорость обработки запросов, усилить уровень защиты информации, повысить эффективность работы служб и подразделений органов внутренних дел Российской Федерации.

Обобщен материал о возможностях моделирования при исследовании процессов формирования террористических структур, разрушения их потенциала вследствие активных воздействий со стороны государства и общества. Воздействия формируются на принципиально различной основе, включая две страте-

гии – жесткую и интеллектуальную, каждая из которых имеет свои преимущества и недостатки в управлении процессами вербовки новых членов экстремистских структур.

Представлены результаты системно-динамического моделирования информационного воздействия и информационного противодействия применительно к сфере борьбы с экстремизмом. Реализация моделей на основе реальных данных показала их адекватность и эффективность при прогнозировании динамики распространения информационных воздействий.

На основе исследования генеральной совокупности (647 поселений России с населением от 10 до 20 тыс. человек) изучены территориальные характеристики распространения информации в наиболее популярной СС ВКонтакте.

На основе кластерного анализа указанные поселения Российской Федерации классифицированы на пять однородных групп, отличающихся скоростями распространения информации в социальных медиа, а, следовательно – показателями «информационного заражения» населения деструктивной информацией. Полученное кластерное деление населенных пунктов страны является важной основой для интерпретации территориальных различий распространения информации, исследования их комплексной обусловленности такими факторами, как организация сетевых сообществ и самих социальных медиа, экономическими, социальными, демографическими, этническими и иными факторами.

Итоги моделирования связаны с обоснованием количественных параметров, позволяющих органам власти, силовым структурам, образовательным и другим заинтересованным организациям относить оцениваемые поселения к разным кластерам по степени восприимчивости населения к информационным влияниям в сети, включая деструктивные воздействия экстремистского характера.

В рамках проведенного исследования найдены наиболее точные алгоритмы и методы выявления деструктивного контента в кратких публикациях и комментариях по трем темам:

- реабилитация нацизма;
- антисемитизм;
- радикальный ислам.

Рассмотренные методы выявления деструктивного контента целесообразно применять в аналитической деятельности соответствующих государственных органов, общественных организаций, сотрудников социальных медиа.

Описанные модели к настоящему времени апробированы, прошли проверку на реальных статистических данных, показали необходимый уровень релевантности, подтвердили свою научную и практическую значимость.

Список литературы

1. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети : модели информационного влияния, управления и противоборства. М. : Физматлит, 2010. 228 с.

2. Минаев В. А., Овчинский А. С., Скрыль С. В., Тростянский С. Н. Как управлять массовым сознанием : современные модели : монография. М. : РосНОУ, 2013. 200 с.

3. Андреев А. А., Бондарь К. М., Минаев В. А. Терроризм и экстремизм: моделирование информационного противодействия : монография. Хабаровск : Дальневосточный юридический институт МВД России, 2020. 251 с.

4. Минаев В. А., Сычев М. П., Бондарь К. М., Вайц Е. В. Системно-динамическое моделирование сетевых информационных операций // Инженерные технологии и системы. 2019. Т. 29. № 1. С. 20–39.

5. Еремин Д. М., Гарцеев И. Б. Искусственные нейронные сети в интеллектуальных системах управления. М. : Издательство МИРЭА, 2004. 75 с.

6. , Чапурин Е. Ю., Разинкин К. А., Плотников Д. Г., Попов А. В. Методы тематического моделирования, их развитие и применение для контента, циркулирующего в региональных онлайн-сообществах / [Е. Н. Телегин и др.] // Информация и безопасность. 2019. Т. 22. № 3 (4). С. 325–344.

7. Гончаров А. А., Чапурин Е. Ю., Белоножкин В. И., Радько Н. М. Развитие методов и построение алгоритмов поиска и классификации деструктивного контента, циркулирующего в социальной сети // Информация и безопасность. 2019. Т. 22. № 3 (4). С. 345–360.

8. Минаев В. А., Реброва А. Д., Симонов А. В. Выявление деструктивного контента в социальных медиа на основе моделей машинного обучения // Информация и безопасность. 2021. Т. 24. № 1. С. 7–20.

9. Минаев В. А., Симонов А. В. Количественная оценка деструктивности больших текстовых массивов в социальных медиа // Информация и безопасность. 2021. Т. 24. № 2. С. 267–280.

10. Минаев В. А., Поликарпов Е. С., Симонов А. В. Применение глубинных нейронных сетей для выявления деструктивного контента в социальных медиа // Информация и безопасность. 2021. Т. 24. № 3. С. 361–372.

11. Социальные сети в России: цифры и тренды // Блог Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2019 (дата обращения: 29.11.2021).

12. Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи // URL: https://guu.ru/files/ dissertations/2016/12/bezbogova_m_s/dissertation.pdf (дата обращения: 29.11.2021).

13. Минаев В. А., Федорович В. Ю. Моделирование информационных воздействий в социальных сетях: территориальный аспект // Вестник Российского

нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 4. С. 8–16.

14. Минаев В. А. Исследование модели динамики деструктивных информационно-психологических воздействий на массовое сознание // Безопасность информационных технологий. 2016. № 4. С. 52–58.

15. Вайц Е. В. Системно-динамический подход к моделированию информационных воздействий // Интернет-журнал «Технологии техносферной безопасности». 2017. № 2. С. 296–306.

16. Grass D., Caulkins J. and others. Optimal Control of Nonlinear Processes. With Applications in Drugs, Corruption and Terror. Springer-Verlag Berlin Heidelberg, 2008. 552 p.

17. Feichtinger G., Hartl R. F., Kort P. M., Novak A. J. Terrorism Control in the Tourism Industry // Journal of Optimization Theory and Applications. 2001. № 108(2), pp. 283–296.

18. Feichtinger G., Novak A. J. Terror and Counter-Terror Operations: A Differential Game with a Cyclical Nash Solution // Forthcoming in Journal of Optimization Theory and Applications. 2008. Vol. 139, pp. 113–120.

Гончар В. В.[1]*,*
заместитель начальника кафедры информационной безопасности учебно-информационного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент

Акиньшин И. С.[2]*,*
заместитель начальника Московского университета МВД России имени В.Я. Кикотя по профессиональному обучению, дополнительному и профессиональному образованию, кандидат экономических наук

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В 2020 И 2021 ГОДУ

В настоящее время интернет следует отнести к одному из основных каналов массовой информации, оказывающий наиболее эффективное воздействие на общество и особенно на молодую его часть, неопределившихся в своих мировоззренческих приоритетах, чьи взгляды на жизнь и смысловые установки еще сформированы и их жизненные пути развития могут сложиться как в сторону принимаемых обществом правил поведения, так и в сторону антисоциальных действий, совершения преступлений, в том числе в сфере IT-технологий.

Проблемы противодействия таким преступлениям стали одними из ключевых проблем настоящего времени.

Выступая в марте 2021 г. расширенной коллегии МВД России, Президент Российской Федерации В. В. Путин отметил, что в настоящее время задачами органов внутренних дел являются эффективный ответ на криминальный вызов IT-преступности, защита граждан и добросовестного бизнеса, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. Президент России обратил внимание на необходимость наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи.

Несмотря на принятые меры в 2020 г. сохранилась динамика существенного роста количества преступлений в рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации – 580,26 тыс., что на 73,4 % превышает показатель предыдущего года

(339,3 тыс.), непосредственно в отчетном периоде зарегистрировано – 510,4 тыс. (+73,4 % к АППГ, 294,4 тыс.). Сложившиеся обстоятельства социально-экономического характера, обусловленные распространением и преодолением последствий новой коронавирусной инфекции COVID-19 создали дополнительные условия для усиления криминальной активности, связанной с использованием IT-технологий.

В массиве уголовных дел данной категории, зарегистрированных в 2020 г., 75,2 % составляют дистанционные хищения, совершенные с банковских карт, с использованием сети Интернет и средств мобильной связи, квалифицируемые по ст.ст. 158 и 159 УК РФ.

В общем числе зарегистрированных преступлений удельный вес IT-преступлений увеличился с 14,5 % в 2019 г. до 25,0 % в 2020 г.

Раскрываемость таких преступлений по-прежнему не высока и по итогам 2020 г. составила 18.6 % (–16 % к АППГ – 22,2 %).

Анализируя информацию из открытых источников, возможно предположить, что доходы, получаемые от IT преступлений могут направляться на финансирование экстремистской и террористической деятельности[1].

Анализируя типичные проблемы расследования таких преступления, следует выделить основные:

1. Не сформирован действенный инструментарий быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.).

Длительность получения ответов составляет от одного до нескольких месяцев.

2. Использование преступниками программного обеспечения, позволяющего избежать (или существенно затруднить) их идентификацию – VPN, TOR, SSL, а также технологий, позволяющих менять IP-адрес пользователя сети «Интернет», создавать динамические или нераспознаваемые IP-адреса, применять технологии «подменных» абонентских номеров посредством IP-телефонии.

3. Недостаточная компьютерная грамотность населения.

В 2020-2021 гг. участились случаи выдачи онлайн-кредитов при установке потерпевшими программ удаленного доступа к электронным устройствам и передаче прав управления преступникам. Преступники, используя методы социальной инженерии, убеждают лицо установить такие компьютерные программы

[1] Город тысячи колл-центров. Почему в России считают Днепр столицей телефонных аферистов // URL: https://strana.news/news/356025-dnepr-stal-tsentrom- telefonnoho-moshennichestva -osnovnye-skhemy-aferistov.html (дата обращения: 18.11.2021); В Киеве телефонные мошенники расположились рядом с офисом СБУ // URL: https://smotrim.ru/article/2620440 (дата обращения: 18.11.2021).

как TeamViewer QuickSupport или аналогичные, после чего получают контроль над устройством потенциального потерпевшего и совершают хищения.

4. Необходимость увеличения числа государственных специалистов и экспертов, имеющих право проводить соответствующие исследования и компьютерные экспертизы. Сегодня практически отсутствуют ведомственные специалисты, способные идентифицировать компьютерную программу как вредоносную методом обратного реверс-инжиниринга. Кроме того, расследование IT-преступлений усложняет длительность производства таких экспертиз и значительная их стоимость при проведении в негосударственных экспертных учреждениях (до нескольких сот тысяч рублей за одну экспертизу при причиненном в большинстве случаев ущербе несколько тысяч рублей).

Решение данных проблем лежит в комплексе законодательных, организационных и научных мер. Кроме того, необходимо активное вовлечение представителей бизнес-сообщества в данную деятельность. Так как в настоящее время финансово-кредитные учреждения для увеличения прибыли всячески упрощают доступ к своим продуктам, не редко пренебрегая вопросами безопасности доступа к ним. Вся полнота ответственности за возможные хищения, например, в результате использования преступниками социальной инженерии, возлагается на клиента, который обязан знать и уметь защищаться от всех угроз.

Необходимо принципиально изменить подход предоставления дистанционных продуктов от «Разрешено все, что не запретил клиент» к «Запрещено все, что не разрешил клиент».

Таким образом, при заключении договора банковского обслуживания клиенту автоматически подключается минимально необходимый, обозначенный им объем услуг. Рискованные услуги, например, возможность дистанционного оформления кредита или подключение дополнительных абонентских номеров будет предоставляться только после идентификации клиента в офисе Банка или иным доверенным способом.

Реализация данных предложений позволит существенно уменьшить количество дистанционных хищений денежных средств, поступления от которых могли идти на финансирование экстремистской и террористической деятельности.

Список литературы

1. Информационно-аналитические материалы следственных подразделений МВД России за 2020 и 2021 гг.

Шевко Н. Р.[1]*,*
доцент кафедры правовой информатики,
информационного права и естественнонаучных дисциплин
Казанского филиала Российского государственного университета правосудия,
кандидат экономических наук, доцент

ИНТЕРНЕТ-ТЕХНОЛОГИИ ПРОТИВ ТЕРРОРИЗМА

В разное время средства массовой информации играли и продолжают играть большую роль в жизни общества. Ознакомление с газетами и журналами в той или иной степени раньше как на территории бывшего СССР, так и практически во всем мире позволяли себе многие. Каждый выбирал себе издание по интересам. Особенностью современного мира является внедрение в жизнь практически каждого человека вне его национальности, территориального нахождения, профессиональных и творческих интересов нового инструмента средств массовой информации – интернета во всем многообразии его представления. Сведения во всемирной сети распространяются молниеносно. И ничто им не является помехой – ни местоположение, ни цензура, ни время суток. Причем в молодежной среде новостям из всемирной паутины доверяют гораздо больше, чем каким-либо иным источникам. Поэтому, на наш взгляд, необходимо более серьезно относиться к информации в виртуальном пространстве и использовать это пространство для реализации патриотического воспитания молодежи, как основы закладки фундамента становления культурного и морально-устойчивого гражданина России.

В 2010 г. интернетом в России пользовались 43,3 млн человек, в 2015 г. – 78 млн человек, в 2017 г. – 87 млн человек, к середине 2018 г. – более 90 млн человек [4], в 2020 г. – 118 млн человек (81 % россиян). Но фактически эти данные немного занижены. Дело в том, что официально дети не могут на себя зарегистрировать аккаунты. Они пользуются учетными данными старших (братьев, сестер, родственников, друзей или родителей). А просматривают информацию в интернете (в основном развлекательного характера) даже дети до года, которые никак не могут попасть в эту статистику.

Среднестатистический пользователь-россиянин проводит в Интернете каждый день более семи часов, т. е. более 40 % бодрствования. Сейчас, во время частичной самоизоляции и работе или учебе в дистанционном формате в некоторых организациях эти цифры значительно увеличиваются.

По данным исследования, центр тяжести интернета постепенно перемещается на восток. Азиатские приложения и веб-сайты занимают все большую долю по активности пользователей со всего мира.

В частности, в последних рейтингах популярных веб-сайтов стало больше азиатских платформ электронной коммерции. Сервис по сбору статистики с сайтов Alexa ставит китайскую платформу Tmall на третье место в мировом рейтинге веб-сайтов, что на 10 позиций выше, чем главный западный конкурент платформы Amazon. В топ-20 самых популярных сайтов рейтинга Alexa входят пять китайских платформ электронной коммерции, четыре из которых принадлежат Alibaba» [3].

Пользователи стали реже доверять различным источникам в Интернете, чаще используют ежемесячные блокировщики рекламы. Однако в среднем каждые 4 из 5 пользователей интернета в возрасте от 16 до 64 лет регулярно игровыми интернет-приложениями. Если использовать этот принцип к мировой численности интернет-пользователей, то общая численность глобального игрового сообщества составляет более 3,5 млрд геймеров. Число онлайн-потребителей видеоконтента тоже растет. Их количество достигает 90 % всех интернет-пользователей.

И как правило, играете ли вы в игры, смотрите ли видео, либо просто читаете новости в ленте, обязательно высвечиваются ролики, причем не всегда позитивного содержания.

Мессенджер Telegram заблокировал 25 358 аккаунтов, связанных с запрещенной в Российской Федерации террористической организацией ИГИЛ. И это только в январе 2020 г. Теперь они появляются с завидной регулярностью. За один день их обнаруживается сотни. За один день их фиксируется порядка одной тысячи.

Массовую блокировку террористических аккаунтов начали в 2016 г. Так в социальной сети Twitter с середины 2015 г. [1] были заблокированы более 125 тыс. аккаунтов, в которых содержались террористические угрозы или пропаганда терроризма. Причем они особенно активизировались в последние месяцы. Первые пару лет за месяц количество заблокированных страниц редко, когда превышало полутора десятков.

Для распространения террористической идеологии используются социальные сети, в интернете действуют сотни сайтов, которые распространяют идеологию террористов. Дальнейшее развитие межведомственного и международного информационного сотрудничества дало положительные результаты по обнаружению и прекращению действия финансовых источников материального обеспечения терроризма. К сожалению, международные террористические организации пытаются активизировать свою деятельность по рекрутированию новых членов, формированию пособнической базы и дальнейшей популяризации своей идеологии – насилия, устрашение населения, межнациональной розни. В 2019 г. по решению органов государственной власти пресечено распространение террористического и экстремистского контента на 50 тыс. страницах в интернете, заблокирован доступ к 16 тыс. зарубежных ресурсов [2].

В 2020 г. [5] не допущено совершения террористических актов, а на стадии приготовления предотвращено 61 преступление террористической направленности, в том числе 41 теракт, нейтрализовано 49 бандитов, в том числе 8 главарей, задержаны 36 главарей банд, 162 боевика и 591 пособник, изъято около 600 единиц огнестрельного оружия. С начала года в стране также разоблачили 55 законспирированных ячеек международных террористов, не допущен въезд 149 иностранных граждан, причастных к экстремистской и террористической деятельности. Также при взаимодействии с Роскомнадзором и правоохранительными органами удалось ограничить доступ к 66,5 тыс. материалов [5] террористического содержания и пресечь деятельность 110 иностранных граждан, осуществлявших их распространение в Сети. Росфинмониторингом заблокированы финансовые активы более 1,2 тыс. лиц, подозреваемых в причастности к террористической деятельности на общую сумму свыше 57 млн руб.

Благодаря четким и слаженным действиям правоохранителей, число терактов в России за последние пять лет сократилось в девять раз. Наибольшую значимость принимает организация системного подхода к пресечению и предупреждению популяризации взглядов террористического характера и недопущения создания пособнической базы террористов.

Нельзя недооценивать повсеместное внедрение интернет-технологий в нашу жизнь и увлеченность молодежи гаджетами и медиа-приложениями. Эта мощная медиа-империя может и должна работать на предотвращение негативного влияния пропаганды и рекрутинговой кампании в ряды террористических и экстремистских организаций, на популяризацию патриотического воспитания, укреплению морального устоя подрастающего поколения, нацеленность на созидание и творчество. Наиболее эффективными методами противодействия рекрутированию являются:

– ликвидация компьютерной безграмотности населения (через проведение тематических занятий в образовательных организациях, создания компьютерных курсов при отделах социальной защиты и т. д.);

– повышение информационной безопасности пользователей, в том числе посредством социальной рекламы);

– проведение социальных акций (видеоролики, мероприятия) по патриотическому воспитанию молодежи;

– создание информационных буклетов (в том числе видеорекламы).

Список литературы

1. Twitter заблокировал более 125 тысяч аккаунтов за пропаганду терроризма // URL: http://elvisti.com (дата обращения: 09.12.2020).

2. В России в 2019 году предотвратили 34 теракта // URL: https://tass.-ru/proisshestviya/7886151 (дата обращения: 05.12.2020).

3. Вся статистика Интернета на 2020 год – цифры и тренды в мире и в России // URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 01.12.2020).

4. Интернет в России 2018: главные цифры // URL: http://security.mosmetod.ru/ (дата обращения: 01.12.2020).

5. Официальный сайт полномочного представителя Президента Российской Федерации // URL: http://szfo.gov.ru (дата обращения: 07.12.2020).

Овчинский А. С.[1],
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

БОРЬБА С ДЕСТРУКТИВНЫМИ ИДЕОЛОГИЯМИ В ЦИФРОВОМ МИРЕ

Значение идеологии в последние годы остается в глубокой тени. Эта тень обусловлена многими разнообразными факторами, среди них: приход информационного общества, вступление в цифровой мир и уже цифровая трансформация, охватывающая все сферы и грани жизнедеятельности.

Идеология как система взглядов, убеждений, ценностей раскрывается в информационных координатах[1] в отношении к происходящему, в интерпретации прошлого, оценке перспектив будущего (фоновый вектор).

Она же выражает и фиксирует идеалы, интересы, намерения. Придавая желаниям и стремлениям людей теоретическое оформление, идеология может воплощаться в программные документы (ресурсный вектор).

Но главное, именно идеология формирует в сознании человека, а зачастую и в массовом сознании обоснование права на определенные действия и поступки, на образ жизни и на образ мыслей. Она может порождать мотивацию и нацеленность, а в критических ситуациях – мобилизацию всех жизненных сил, вплоть до самопожертвования (реактивный вектор) (рис. 1).

Рис. 1. Идеология в проекциях

[1] © Овчинский А. С., 2021.

Также как технологические достижения могут быть использованы во благо и во зло, в русле идеологии могут накапливаться как конструктивные, так и деструктивные потенциалы. Идеология может быть направлена на созидание, прорыв к новому или на защиту традиционных ценностей. Но она может оправдывать и даже обосновывать разрушительные действия, насилие и жестокость, вести к деградации и хаосу.

Именно в русле определенных идеологий накапливаются потенциалы деструктивной социальной психологической энергии. Разрядка потенциалов этой энергии проявляется в террористических актах, экстремистских выступлениях, гражданских столкновениях, криминальных разборках.

Об энергии, необходимой для действий и поступков, русские философы писали еще в начале двадцатого века. Питирим Сорокин называл социально психологическую энергию высшей из всех видов энергий. Советские ученые вплотную подошли к оперированию понятием «социальная энергия», которая соответствует самой высокой, то есть общественной форме движения материи. Сегодня в условия возрастающей интенсивности воздействия на массовое сознание можно утверждать, что эта энергия связана с информацией.

Потенциалы социальной психологической энергии порождает информация, которая возникает в сознании человека, как реакция на получаемые сообщения и сигналы (реактивная информация).

Одновременно потенциалы этой энергии формируются той информацией, которая фиксируется и накапливается как в памяти людей, так и на определенных носителях (ресурсная информация).

В образование как конструктивных, так и деструктивных энергоинформационных потенциалов вносит вклад и фоновая информация, которая, отражая окружающую реальность, может обходить защитные функции сознания.

Глубинные истоки деструктивных идеологий можно увидеть в религиозных культах с человеческими жертвоприношениями. Страх, террор в течение многих веков был основным психологическим оружием завоевателей и поработителей. Главным элементом подготовки убийц на Ближнем Востоке была идеология, в русле которой считалось, что убивать «неверных» угодно Богу. Более того, гибель исполнителя террористического акта якобы приводила его душу непосредственно в райские кущи.

Из исторических хроник известно, что в арабских странах, еще в XII в. будущих смертников усыпляли, перевозили в специально оборудованные оазисы, где они в прекрасных садах предавались всем возможным усладам. Их обильно кормили, поили винами, угощали сладостями, их услаждали специально подготовленные гурии. После пробуждения люди считали, что побывали в раю, и опять туда стремились попасть, совершая заказные убийства и жертвуя своими жизнями.

В настоящее время для формирования и накопления потенциалов деструктивной энергии уже не требуется ни декораций, ни хлопотных инсценировок. Достаточно технологий дополненной реальности, геймификации, глубоких фейков, то есть технологий, которые погружают человека в специально сконструированный виртуальный мир.

В деструктивных идеологиях отражаются идеи мальтузианства, по ограничению и сокращению населения Земли. Сегодня эти идеи находят реализацию в акциях «зеленых» с призывами не иметь детей, в изощренных акциях психодемографической информационной войны.

Деструктивные энергоинформационные потенциалы накапливались и продолжают подпитываться концепциями социодарвинизма, теориями высших и низших рас, радикальным национализмом. Фашистская идеология была осуждена в свое время, но возрождается в разных странах в разных формах.

В целом идеология – это многогранное явление. Можно говорить о политических, национальных, классовых идеологиях. В противодействии деструкции коснемся потенциалов, которые содержат три основные мировые идеологии: либерализм, консерватизм, социализм.

Либерализм, сформировавшийся на заре капитализма, приоритетами провозгласил права человека, человека активного, деятельного, стремящегося к благополучию и обогащению. В западноевропейской философской традиции человек занимал центральное место, или замещая Бога, или его отрицая.

Но в реальности человек оказывался далеко несовершенным, а иногда и порочным. Человек мог совершать не просто преступления, но и злодеяния, и современный либерализм, навязывая миру свои правила жизни, уже дошел до гендерного многообразия, когда свобода выбора сводится к выбору своей половой принадлежности.

Как альтернатива либерализму сформировался консерватизм – идеология защиты традиционных ценностей. Если либерализм формирует человека потребителя, то в русле консервативной идеологии воспитывается личность человека-защитника.

Об этом говорил В. В. Путин на Валдайском форуме 2021 года. Более того, он отметил представление об идеологии умеренного консерватизма как наиболее отвечающий интересами российского общества на современном этапе. Президент цитировал русского философа Николая Бердяева, отмечая, что разумный консерватизм – это не сдерживание движения вперед и вверх, а защита от движения назад и вниз, защита от деградации и хаоса.

Но, только защищаясь, трудно ожидать творческих прорывов и побед, в частности, в борьбе с социальной деструкцией. Нужно обратить внимание на третий вектор мировых идеологий социализм, а в перспективе и коммунизм. Здесь отдается приоритет справедливости, общинности, коллективизму.

Следует отметить, что и коммунистическая идеология содержала деструктивные элементы, оправдывала право на насилие. Но насилие ради освобождения от капиталистической эксплуатации и колониального гнета. Эта идеология была скомпрометирована идеей мировой революции.

В то же время идеология, которая являлась государственной в Советском Союзе, была направлена на формирование, на воспитание человека-творца. Так и было обозначено в программных документах партии.

Можно по-разному относиться к советскому периоду нашей истории, но сложно отрицать, что творческий потенциал идеологии находил реализацию в весьма эффективной системе образования, подготовке высококвалифицирован-

ных специалистов, в достижениях советских ученых. Этот потенциал дает о себе знать и сейчас. Слова шуточной песни семидесятых годов прошлого века «Зато мы делаем ракеты» наполняются новыми смыслами после успешных испытаний наших гиперзвуковых ракет, после поражений высокоскоростных космических объектов. И это дает нам ощущение определенной защищенности от военных угроз.

Но все-таки основные угрозы несут вредоносные деструктивные воздействия на сознание людей. Объективные исследования сетевых коммуникаций показывают, что многие граждане нашей страны в той или иной мере вовлечены в деструктивную деятельность. Более 60 % из них это молодежь (подростки, школьники, студенты). Отношение к стране, к политике у них формируется в условиях жестких информационных войн: ментальных, смысловых. Так, в нарицательные девяностые смысловой вакуум наполнялся криминальной идеологией, обосновывающей право на преступную деятельность.

Терроризм, экстремизм, расстрел учащихся, как и любые подобные деяния зарождаются в сознании. Но, чтобы совершить насильственный акт, необходимо накопить потенциалы деструктивной энергии. Эти потенциалы формируются из информации, которую генерирует сознание человека.

Разрядка деструктивных потенциалов (рис. 2) приводит к действиям: человек надевает пояс шахида и подрывает себя, выходит на протестный митинг и бросает камень, берет ружье и идет расстреливать школьников.

Результат подобных действий – это уже то или иное событие: десятки убитых и раненных на станции метро, травмы полицейских, гибель и ранения учащихся.

Сообщения об этих событиях с их интерпретацией порождает в сознании одних людей возмущение, скорбь, страх, в сознании других одобрение, восхищение, пример для подражания.

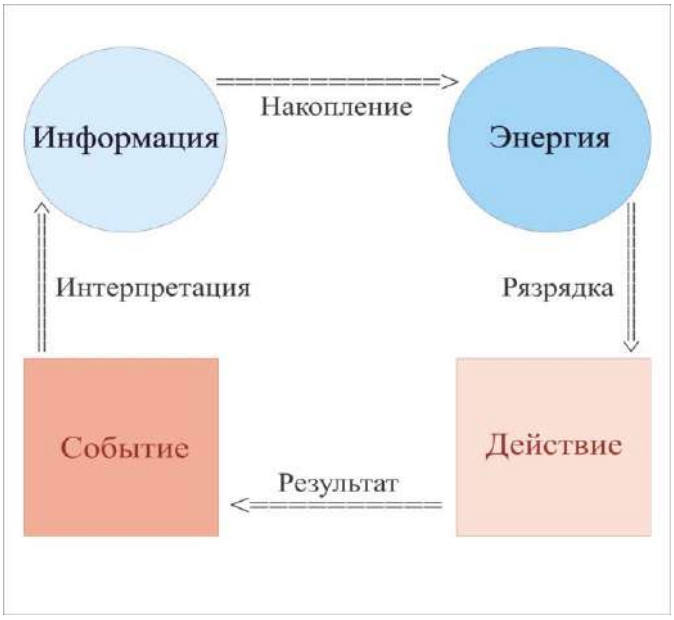


Рис. 2. Энергоинформационные трансформации в социальных процессах и явлениях

Интернет-коммуникации и социальные сети не только распространяют «со скоростью света» данные и сведения. Они часто задают такие ключи интерпретации деструктивных событий, которые требуются заказчикам и вдохновителям этих событий. Так, схема замыкается, мы имеем систему энергоинформационной трансформации, в которой протекает жизнь человека.

Действия и события материального мира порождают информацию и энергию идеального мира – внутреннего мира человека. Также возникновение информации и накопление энергетических потенциалов в идеальном мире порождают действия и события в материальном мире и наоборот.

Как разорвать порочные круги зарождения, накопления и реализации потенциалов социальной деструкции? Как вообще управлять социальными процессами, обеспечивать безопасность информационных сфер? Цифровая трансформация выводит нас на цифровые платформы: программные, прикладные, инфраструктурные.

Необходимо создать цифровые функциональные платформы, накапливающие требуемые энергоинформационные потенциалы и цифровые инструментальные платформы, направляющие потоки социально психологической энергии в требуемое русло. Речь идет о платформах, с помощью которых будут созданы механизмы управления переходами из мира мыслей и желаний в мир действий и событий и обратно.

Цифровые платформы – это комплекс взаимосвязанных алгоритмов получения, накопления и обработки данных в частности с построением цифровых профилей лиц, требующих, например, профилактических учета и воздействий. Цифровые платформы – это и комплекс коммуникационных серверов – механизмов формирования и адресной рассылки сообщений – управляющих воздействий. Цифровые платформы должны включать программные комплексы инициативной и предиктивной оперативно-разыскной аналитики, алгоритмы, которые построены на возможностях самообучающихся нейронных сетей[2].

Технологически это решаемая задача. Проблема в ментальном, содержательном, смысловом наполнении этих платформ. И проблема эта обостряется тем, что мы стоим на пороге еще одного технологического перехода – создания виртуальных миров.

Виртуальные миры возникли не вчера, они созревали с геймификацией[3], как социальной технологией, то есть индустрией компьютерных игр, с технологиями дополненной реальности, когда человек надевает очки-шлем, подключает к телу датчики и оказывается в виртуальном мире. Цукерберг уже презентовал технологию мета и свою метавселенную. На широкую арену выходят дипфейки – глубокие фейки, построенные на машинном обучении, когда сконструированные масс-медиа события уже практически невозможно отличить от реальных.

Еще относительно недавно Интернет-коммуникации и социальные сети стали захватывать людей, но уже в ближайшем будущем мы столкнемся или окажемся в виртуальных мирах.

Без четких идеологических посылов мы оставляем тот смысловой вакуум, который позволяет выстраивать виртуальный мир, то есть виртуальное настоящее, виртуальное прошлое, виртуальное будущее, например, на деструктивных

основаниях, ведущих к деградации и хаосу, или на либеральных догматах, трансформирующихся в приоритет человеческим порокам.

Реальная жизнь с ее ценностями уже автоматически уходит на второй план по мере погружения в виртуальные миры. Это опасная ловушка для огромного количества людей.

Но главная угроза – не сам виртуальный мир, а его смысловое наполнение, то есть опять же идеология. Пора идеологию выводить из тени. В начале девяностых государственная идеология у нас в стране вообще была запрещена Конституцией, написанной под диктовку американских кураторов. Наш отечественный опыт идеологического воспитания остается не востребованным. Сегодня рассказы о комсомольцах, пионерах, октябрятах, воспринимаются молодыми людьми примерно также как мифы о героях Древней Греции.

Говоря об управлении энергоинформационными трансформациями, порождающими и сопровождающими социальное движение, можно отметить, что цифровые функциональные и цифровые инструментальные платформы должны опираться на ясную государственную идеологию (рис. 3), они должны включать пропаганду, агитацию, адресные целенаправленные воспитательные воздействия на сознание людей. Идеология должна объединять народы нашей страны, она должна быть привлекательной для жителей других стран и регионов.

Рис. 3. Идеология как база ментального наполнения цифровых платформ управления социальными процессами

Так, видятся принципиальные возможности повышения эффективности противодействия социальной деструкции, экстремизму и терроризму в информационных сферах.

Список литературы

1. Овчинский А. С., Борзунов К. К., Чеботарева С. О. Информационные координаты. Управление. Противоборство. Безопасность.М. : Горячая линия Телеком, 2018.

2. Овчинский А. С. Цифровые платформы оперативно-разыскной профилактики преступлений // Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов. М. : Инфра-М, 2021.

3. Сундиев И. Ю., Смирнов А. А. Оперативно-розыскная характеристика использования технологии геймификации в экстремистской и террористической деятельности // Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов. М. : Инфра-М, 2021.

Дош Н. А.[1]***,***
директор по рискам
Ассоциации участников Мастеркард

ОБЗОР АКТУАЛЬНЫХ МИРОВЫХ ПРОБЛЕМ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Преступники непрерывно осваивают современные технологии и направляют их в криминальное русло. В настоящее время преступники умеют многое – они достаточно качественно подделывают сайты государственных органов, организаций здравоохранения, благотворительных организаций и фондов, интернет-магазинов и банков. Благодаря слитым в сеть персональным данным мошенники получили возможность связываться с потенциальными жертвами – убеждать, запугивать и угрожать.

В условиях распространения новой коронавирусной инфекции в мире преступники разработали и используют множество новых либо хорошо забытых старых схем, направленных на получение выгоды от их совершения.

Такой вид атак на устройства самообслуживания как «скимминг» (копирование данных на магнитной полосе банковской карты) для Российской Федерации по объективным причинам стремится к нулю, но в других странах этот метод активно используется криминальными группами для кражи денежных средств. В последнее время интерес для мошенников представляют не только банкоматы, но и другие устройства самообслуживания, где используются банковские карты. «Скимминговые» устройства были выявлены в автомате по продаже железнодорожных билетов и на автоматической заправочной станции.

Еще один негативный зарубежный тренд, который фиксируется на сегодняшний день, – это подрыв банкоматов с помощью газа или взрывчатки. Данный вид атаки характеризуется огромными сопутствующими разрушениями и периодической гибелью как самих преступников, пытающихся подорвать банкомат, так и случайных прохожих, оказавшихся неподалеку от места взрыва. Для понимания масштабов проблемы на примере Германии стоит отметить, что за неполный 2020 год на территории этой страны зафиксировано более 400 подрывов банкоматов. Такого рода цифра демонстрирует нам еще одну большую проблему в Европе, связанную с достаточно свободным доступом криминальных элементов к взрывчатым веществам и их использованием в людных местах. Это тем более опасно, учитывая последствия подрывов банкоматов на территории европейских стран.

Рассмотрим наглядно.

Ассоциация участников МастерКард

АТАКИ НА БАНКОМАТЫ

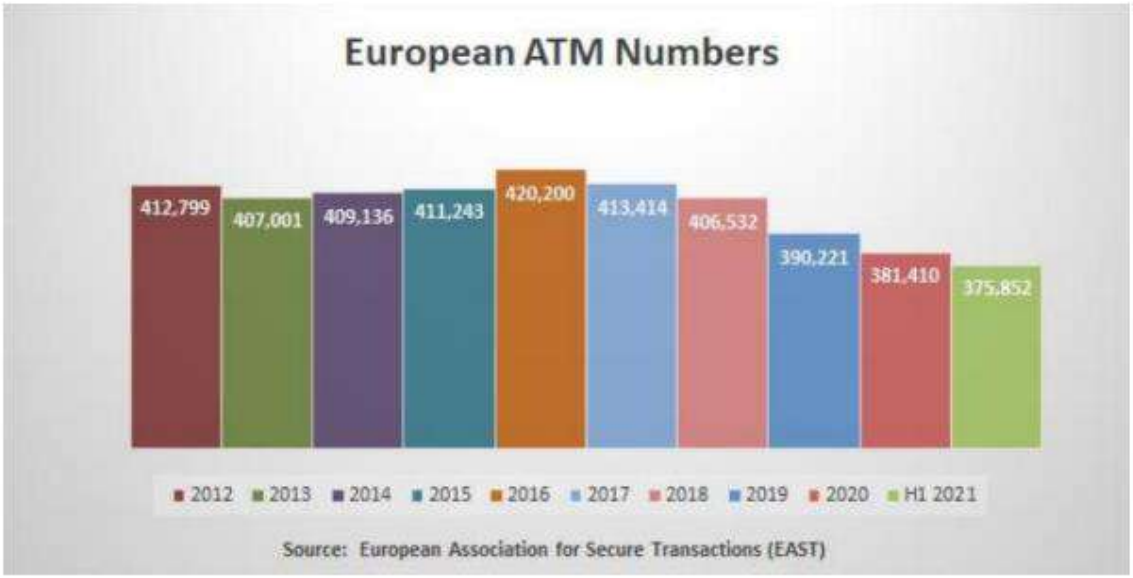


Рис. 1. Атаки на банкоматы

Ассоциация участников МастерКард

АТАКИ НА БАНКОМАТЫ

Рис. 2. Атаки на банкоматы

Рис. 3. Атаки на банкоматы

Рис. 4. Атаки на банкоматы

INVESTMENT SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,359	2,026	3,425	3,364	3,723	5,235	6,864	84%	31%
Number of payments	3,675	4,261	7,126	7,097	9,492	13,761	20,152	112%	46%
Total value of losses	£20.8m	£29.3m	£43.4m	£51.9m	£55.2m	£79.9m	£107.7m	95%	35%
Total subsequently returned to the customer	£1.4m	£2.5m	£2.9m	£9.4m	£15.1m	£33.9m	£44.3m	193%	31%

PURCHASE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	21,483	31,138	35,472	37,864	37,516	41,204	52,348	40%	27%
Number of payments	27,011	39,685	44,252	48,868	47,768	54,834	68,763	44%	25%
Total value of losses	£19.4m	£26.9m	£27.9m	£31.1m	£27.1m	£30.0m	£37.7m	39%	26%
Total subsequently returned to the customer	£1.6m	£2.6m	£2.7m	£6.9m	£6.8m	£9.6m	£11.0m	63%	15%

Рис. 5. Дистанционный фрод

Ассоциация участников МастерКард

ДИСТАНЦИОННЫЙ ФРОД

IMPERSONATION: POLICE/BANK STAFF

IMPERSONATION: POLICE/ BANK	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,947	3,512	4,242	6,846	8,222	13,245	18,816	**129%**	**42%**
Number of payments	3,196	5,507	10,056	12,204	14,478	27,510	39,246	**171%**	**43%**
Total value of losses	£22.2m	£34.3m	£35.4m	£48.7m	£36.7m	£59.9m	£84.7m	**131%**	**41%**
Total subsequently returned to the customer	£6.9m	£12.9m	£11.2m	£26.1m	£23.4m	£36.1m	£48.7m	**108%**	**35%**

CEO FRAUD

CEO	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	347	256	340	336	241	596	207	**-14%**	**-65%**
Number of payments	478	353	487	475	361	770	310	**-14%**	**-60%**
Total value of losses	£8.0m	£6.8m	£7.9m	£9.8m	£4.7m	£5.7m	£6.5m	**37%**	**14%**
Total subsequently returned to the customer	£2.2m	£2.1m	£2.1m	£1.7m	£2.2m	£1.7m	£3.0m	**36%**	**72%**

Рис. 6. Дистанционный фрод

Ассоциация участников МастерКард

ВИРУСЫ ВЫМОГАТЕЛИ

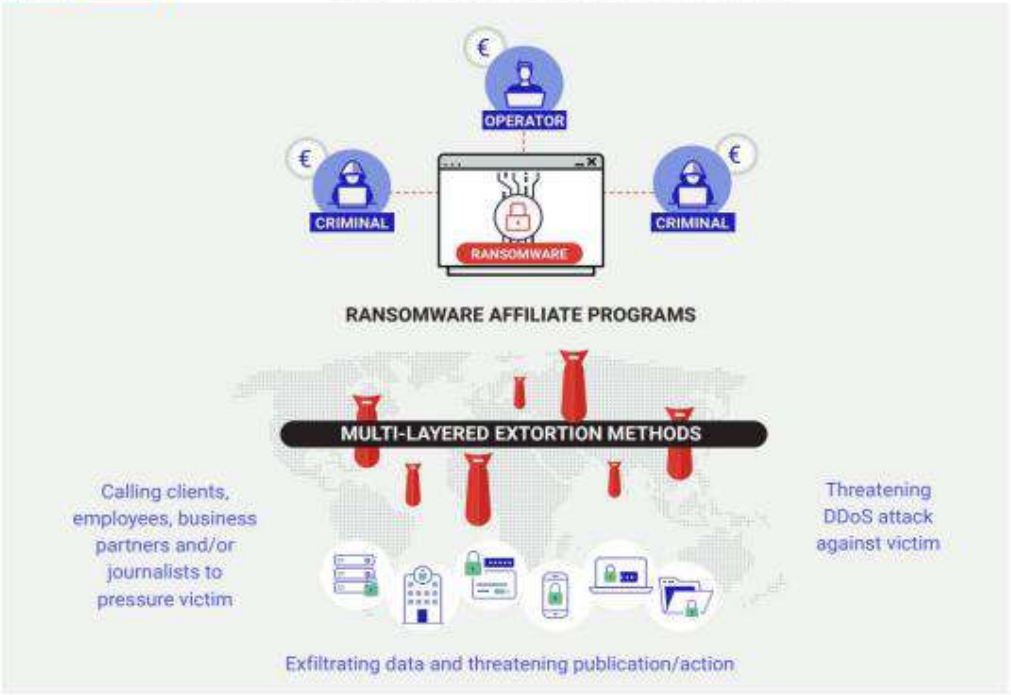


Рис. 7. Вирусы вымогатели

Борзунов К. К.[1]**,**
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ

Терроризм может носить характер боевых операций и актов, в ходе которых наносится существенный ущерб объекту или субъекту нападения или осуществляется физическое уничтожение его. Терроризм может носить характер кибератак и акций, в ходе которых наносится ущерб объектам критической инфраструктуры от блокирования до выхода из строя. В современных условиях терроризм может носить характер ведения полномасштабной информационной войны или информационно-психологических воздействий (операций) в отношении населения, социальных слоев или отдельных личностей, являющихся значимыми представителями в определенной сфере (культуры и духовности, науки, экономики или производства, политики и т. д.).

Экстремизм, прежде всего, связывают с насильственным изменением основ государственности (конституционного строя). И в то же время экстремизм вбирает в себя как составную часть терроризм. Особенность экстремизма связывается, как правило, с обоснованием и оправданием терроризма; с пропагандой исключительности – превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности; с ложными обвинениями руководителей страны и представителей власти и органов местного самоуправления, а также значимых лиц политических, общественных и религиозных объединений; с возбуждением социальной, расовой, национальной или религиозной розни и подстрекательством к неповиновению властям.

Следует отметить, что в рамках терроризма и экстремизма можно выявить особый процесс возникновения, развития и распространения различных идеологий (расизма, национализма, религиозного фанатизма…, т. е. насилия) – «питательной» среды вовлечения людей в террористическую и экстремистскую деятельность и превращения их в исполнителей замыслов лидеров террористических и экстремистских организаций (нелегальных, подпольных).

Историческая практика социальных преобразований, реформирования государственных структур свидетельствует о довольно распространенном «скатывании» к революционным методам, базирующихся на идеологии насилия (диктатуры), в силу наличия опасений за результаты преобразований и реформирования, а также возникновения противодействия определенной части общества и в целом государства…

Кроме всего прочего, возникла, существует и поддерживается специфическая сфера финансирования терроризма и экстремизма теми, кто заинтересован

в преобразовании социального и государственного устройства мира в собственных интересах, не учитывающих интересы многочисленных и разнообразных отдельных социальных слоев, народов и, в конце концов, населения мира…

В области информационно-аналитического обеспечения противодействия терроризму и экстремизму возникают представления об объектах, которые требуют выявления и исследования: центры планирования и непосредственного ведения информационно-психологических воздействий (операций) или экстремистских акций и террористических актов (заинтересованная сторона); источники финансирования; центры разработки методов, способов и средств ведения информационно-психологических воздействий (операций); центры подготовки террористов и террористических актов; производители или источники оружия, боеприпасов, вооружения; исполнители (организованные группы во главе с лидером-руководителем: непосредственного исполнения, технического обеспечения и прикрытия, непосредственного финансирования); объекты или субъекты нападения (воздействия).

Составляющие информационно-аналитического обеспечения (ИАО) в области предупреждения (профилактики) террористической и экстремистской деятельности: мониторинг средств массовой информации (СМИ) в целях выявления подготовки и проведения конкретных информационно-психологических воздействий (операций); мониторинг (выявление) объектов или субъектов нападения (воздействия); мониторинг телекоммуникационных сетей в целях выявления активности организационной деятельности групп непосредственного исполнения, технического обеспечения и прикрытия, непосредственного финансирования; выявление замыслов организованных групп и признаков подготовки к определенным экстремистским акциям (в частности информационно-психологическим воздействиям (операциям)), террористическим актам в отношении выбранных уязвимых объектов или субъектов…

Составляющие ИАО в области раскрытия и расследования событий террористической и экстремистской направленности: выявление и фиксация лиц, представляющих собой относительно устойчивые группировки террористической и экстремистской направленности, по мониторингу телекоммуникационных сетей и в ходе оперативно-розыскной деятельности; накопление и анализ фактографической информации о событиях террористической и экстремистской направленности по мониторингу телекоммуникационных сетей, в ходе криминалистической и оперативно-розыскной деятельности; выявление и фиксация событий и лиц, связанных с организационной, финансовой и технической поддержкой террористических актов и экстремистских акций по мониторингу телекоммуникационных сетей, в ходе криминалистической и оперативно-розыскной деятельности.

Составляющие ИАО в области противоборства с идеологией терроризма и экстремизма, вербовке лиц в организованные группы террористической и экстремистской направленности: мониторинг Интернет-пространства на предмет выявления информационных ресурсов по экстремистской и террористической идеологии; мониторинг скрытых платформ телекоммуникационных сетей на предмет выявления информационных ресурсов целенаправленного изучения и

овладения экстремистской и террористической идеологией; мониторинг скрытых платформ телекоммуникационных сетей на предмет выявления чатов, используемых для вербовки лиц в организованные группы террористической и экстремистской направленности; мониторинг скрытых платформ телекоммуникационных сетей на предмет выявления информационных ресурсов целенаправленного изучения и овладения методами, средствами и способами террористических актов и экстремистских акций.

Возможно создание специальных (отдельных) составляющих ИАО в области противодействия финансированию террористических актов и экстремистских акций, а также снабжению необходимыми денежными средствами завербованных организованных групп в ходе подготовки и реализации конкретных террористических актов на объектах и экстремистских акций по отношению к субъектам: выявление каналов финансирования центров планирования террористических актов и экстремистских акций; выявление каналов финансирования центров подготовки террористов и террористических актов; выявление каналов финансирования центров разработки методов, способов и средств ведения информационно-психологических воздействий (операций); выявление каналов поступления денежных средств на этапе подготовки и реализации конкретных террористических актов на объектах и экстремистских акций по отношению к субъектам.

Анализируя составляющие ИАО в области предупреждения (профилактики) террористической и экстремистской деятельности, можно отметить следующее.

Во-первых, возможность выявления резко ограничивается, чем выше уровень объектов оперативного интереса, для подразделений ИАО органов внутренних дел.

Во-вторых, по-видимому, первоначально удастся зафиксировать активность средств массовой информации (СМИ) по определенному вопросу (проблеме), выявить потенциальный объект или субъект экстремистской акции и оценить степень уязвимости. На основе анализа больших данных возможно выдвижение гипотез о том, будут ли применяться какие-либо боевые операции, кибератаки или информационно-психологические воздействия (операции). Мониторинг телекоммуникационных сетей возможно выявит некоторое повышение активности организационной деятельности групп соответствующей направленности. Сопоставление получаемых данных во времени и пространстве приведет к гипотезе о вероятности осуществления определенного террористического акта или экстремистской акции. Внимание следует обращать на события, которые характеризуются чрезвычайно низкой или вполне высокой вероятностью.

В-третьих, аналитическая деятельность должна осуществляться на фоне проведения оперативно-розыскных мероприятий, учитывающих результаты непрерывной текущей аналитической работы, упомянутой ранее. И реальная картина событий возникает как результат оперативно-розыскной деятельности, высокая эффективность которой обеспечивается аналитической деятельностью.

Анализируя составляющие ИАО в области в области раскрытия и расследования событий террористической и экстремистской направленности, можно отметить следующее.

Мониторинг открытых социальных сетей и скрытых чатов в телекоммуникационных сетей, используя методы киберразведки и компьютерной разведки, возможно даст некоторые предположения об относительно устойчивых группировках террористической и экстремистской направленности. Более детальный анализ связей лиц, контента их общения позволит конкретизировать устойчивость организованных групп и их направленность. Используя методы аналитической разведки в отношении фактографических данных, можно прийти к более глубоким и объективным выводам, адекватным представлениям о реальных событиях террористических актов и экстремистских акций, их предшествующей подготовки, роли участников событий.

Анализируя составляющие ИАО в области противоборства с идеологией терроризма и экстремизма, вербовке лиц в организованные группы террористической и экстремистской направленности, можно отметить следующее.

Определение расположения в Интернет-пространстве информационных ресурсов и установление их предназначения, выявление действующих чатов по вербовки лиц в организованные группы террористической и экстремистской направленности осуществляется посредством комбинирования методов киберразведки и компьютерной разведки. Причем следует отметить, что данный вид деятельности носит определенно характер комбинированный, в котором сочетаются одновременно и оперативно-разыскные мероприятия (технического плана), и информационно-аналитические мероприятия. Подобного рода комбинированная деятельность позволит наметить, подготовить и реализовать при определенных условиях планы по аппаратно-программной ликвидации выявленных объектов, используемых в целях распространения и приобщения к идеологии терроризма и экстремизма, вербовки лиц в организованные группы террористической и экстремистской направленности.

В ходе решения задач по противодействию терроризму и экстремизму информационно-аналитические подразделения органов внутренних дел должны быть нацелены, прежде всего, на выявление:

– враждебных и агрессивных сторон по отношению к государству, населению, социальным слоям и отдельным значимым представителям в определенной сфере (культуры и духовности, науки, экономики или производства, политики и т. д.);

– источников финансирования;

– уязвимых объектов и субъектов террористических и экстремистских устремлений;

– сетевых организационных структур террористических и экстремистских организаций – взаимосвязанных центров: планирования, финансирования и подготовки террористических актов и экстремистских акций; разработки методов, способов и средств проведения террористических актов и экстремистских акций; вербовки групп исполнителей, организационно-финансовой и организационно-технической (боевой) поддержки;

– целей и задач центров планирования и подготовки террористических актов и экстремистских акций, а также групп исполнителей террористических актов и экстремистских акций;

– локальных финансовых каналов поступления денежных средств группам исполнителей террористических актов и экстремистских акций, группам организационной и технической (боевой) поддержки.

Однако, развивая теоретические представления об информационно-аналитическом обеспечении противодействия терроризму и экстремизму, нельзя не отметить следующие моменты.

В настоящее время в организационном плане для органов внутренних дел есть существенные ограничения для реализации отдельных видов мониторинга, выявления некоторых центров, объектов и субъектов террористических и экстремистских посягательств. В меньшей мере эти ограничения касаются информационно-аналитического обеспечения в области в области раскрытия и расследования событий террористической и экстремистской направленности. Преодолимые в организационном плане ограничения для органов внутренних дел существуют, пожалуй, для информационно-аналитического обеспечения в области противоборства с идеологией терроризма и экстремизма, вербовке лиц в организованные группы террористической и экстремистской направленности.

В практическом плане реализации информационно-аналитического обеспечения противодействия терроризму и экстремизму в виде конкретных аппаратно-программных комплексов существует известная проблема отсутствия Научно-производственного центра развития (разработки) информационных технологий, кооперированного с системой учебных заведений (организаций) в структуре МВД России. Причем такой Центр должен соответствовать весьма высоким требованиям, диктуемым сложившимся состоянием преступности и борьбой с ней в Российской Федерации.

Уместно еще раз подчеркнуть, что профессорско-педагогический состав кафедр учебных заведений в структуре МВД России подобного рода задачи не решит с силу отсутствия возможностей и работоспособных научно-производственных подразделений.

Лонщакова А. Р.[1]*,*
доцент кафедры оперативно-разыскной деятельности
органов внутренних дел
Уфимского юридического института МВД России,
кандидат юридических наук, доцент

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ ПРИ ОТРАБОТКЕ УРОВНЕЙ ЗАЩИТЫ ИНФОРМАЦИИ

В статье рассматриваются особенности выявления оперативно-значимой информации при отработке уровней защиты информации. Обосновывается вывод о том, что комплексные системные механизмы выявления и противодействия цифровым атакам являются перспективными инструментами для их эффективного контроля и нейтрализации, в том числе, при нейтрализации атак по делам об экстремизме и терроризме в информационной сфере. Материал подготовлен на основе анализа эмпирического материала – по специально разработанной анкете нами изучено более ста сорока четырех киберинцидентов[2].

При поиске и анализе неструктурированных данных – в целях выявления оперативно-значимой информации особое внимание следует уделять методам выявления, фиксации, изъятия и исследования цифровых значимых следов: изучению программного обеспечения для их анализа и исследований на различных точках, анализа сетевого взаимодействия, инструментов и программных продуктов извлечения информации с исследуемых операционных систем, жестких дисков и энергозависимой памяти, средств изучения машинных носителей информации, установленного шифровального программного обеспечения и др.

По результатам нашего исследования инициаторы киберинцидентов профессионально применяли в своей деятельности высокотехнологичные специальные программно-аппаратные средства, инструменты, системы удал енного доступа, технику, криптографические программные продукты и др. инструменты, методики, тактические приемы и технологии, в том числе с использованием социальной инженерии. В связи с этим, полагаем, особое значение имеет анализ уровня защиты информации (данных) с учетом ее трех агрегатных состояний: в покое, в движении, в работе (использовании). Для выявления значимой информации, ее документирования, использования при доказывании инцидента нужны маркеры о работе с тремя состояниями информации (данных).

Инструментами для решения этих задач являются следующие системы защиты информации: DAM-системы, DCAP- системы, DLP-системы и др.

Рассмотрим отдельные особенности работы с данными системами защиты информации.

---

[2] Материалы предоставлены: начальником отдела информационной безопасности «Сёрч-информ» Алексеем Дроздом; экспертом по кибербезопасности Дмитрием Галовым; ведущим консультантом отдела мониторинга рисков Управления по противодействию отмыванию доходов Росфинмониторинга Сергеем Нечушкиным; экспертом по кибербезопасности Сергеем Волдохиным.

Механика инцидента состоит из трех последовательно сменяющих друг друга операций. Его механику можно раскрыть на примере анализа типовых случав:

– информация может быть выгружена из базы данных;

– информация может быть скопирована и сохранена в виде файла;

– информация (файл) может быть отправлена за пределы системы.

Например, нужна информация с персональными данными. Чтоб ее выгрузить, необходимо сформировать отчет. Инцидент начинается с того, что злоумышленник нажимает кнопку, чтоб сформировать отчет. Этот отчет надо выгрузить в файл, то есть сделать экспорт файла. На этих этапах идет взаимодействие между компьютером и системой: создать и выгрузить отчет. Эта область DAM-систем.

Файл выгрузили, он появился на компьютере либо в сетевой папке. У нас есть файл, который находится в состоянии покоя. С файлами, которые находятся в состоянии покоя работают DCAP- системы.

Далее файл необходимо переправить (вынести) за периметр: по почте, через мессенджеры, на флешке. Информация пришла в движение. За работу с информацией в движении отвечают DLP-системы.

Исследуя механику движения данных (информации) инцидента можно не только выявить инцидент, но и предотвратить его. Потому что все перечисленные системы умеют не только проводить аудит, но и осуществлять контроль и блокировку информации при подозрительных действиях, например, делам об экстремизме и терроризме в информационной сфере.

Линия жизни инцидента с этапа формирования намерений и до стадии маневрирования информацией важна для понимания его механизма. Когда информация покидает защищенный периметр начинают работу DLP-системы (когда информация пришла в движение).

На стадии накопления информации работаю DLP-системы и DCAP-системы.

Эффективнее выявлять оперативно-значимую информацию на стадии формирования намерений. Отдельные особенности имеет тактика работы с группами риска.

У каждого киберинцидента есть имя и фамилия. Еще у каждого киберинцидента есть предыстория. У каждого киберинцидента есть причины и условия. Если анализировать результаты анализа киберпроисшествий (киберпреступлений) – стадию формирования намерений, то мотивами преступлений по делам об экстремизме и терроризме в информационной сфере явились два мотива: корыстный и идеологический.

Выявление и фиксация оперативно-значимой информации, в том числе, и цифровых следов, является связующим звеном стратегии защиты.

Оптимальная стратегия защиты – зафиксировать инцидент в настоящем, тщательно расследовать его прошлое, чтобы разработать меры для предотвращения таких инцидентов в будущем.

Анализ прошлого инцидента позволяет отработать причины и условия, которые способствовали его наступлению и разработать меры предотвращения и профилактики инцидентов. Но не через блокировку, а через перестройку систе-

мы. То есть таким образом, что у людей даже не было возможности совершать злонамерения. Важен точный контроль действий и совокупность систем защиты.

В современных условиях для обеспечения информационной безопасности необходимо создать единую комплексную инфраструктуру для защиты всего киберпространства. Злоумышленники пытаются преодолеть, нейтрализовать систему защиты и получить доступ к охраняемой информационной среде, используя для этих целей современные технические возможности и социальную инженерию.

Практики расследования киберинцидентов интегрируют инструменты для выявления значимой информации (инструменты для мониторинга) и раскрывают типовые способы подготовки, совершения цифровых атак.

В этой связи, по результатам анализа эмпирического материала, актуальными являются отдельные типовые практики расследования инцидентов:

– хищение персональных данных: сработала политика безопасности по копированию персональных данных на внешнее устройство – флеш-карту. *Инструментами для выявления значимой информации (инструментами для мониторинга) явились следующие:* использование и анализ DLP-системы, анализ информации в почте, в мессенджерах показал, что злоумышленники действовали совместно в составе группы. Причастные лица выявлены, осуждены.

– распространение информации об экстремизме и терроризме через логистическую компанию*:* сработала политика по словарю – сообщения топ-менеджера в социальных сетях содержали кодовое слово и автомобильный номер. *Инструментами для выявления значимой информации (инструментами для мониторинга) явились следующие:* анализ DLP-системы, анализ переписок сотрудников компании выявил, что коды были номерами машин из корпоративного автопарка. DLP-система нашла совпадение по ключевым словам. Причастные лица были выявлены.

– шантаж*:* через сеть «ВКонтакте» поступали анонимные письма. В письме угрожали обнародовать проступки и требовали совершить незаконные преступные действия. *Инструментами для выявления значимой информации (инструментами для мониторинга) явились следующие*: анализ аккаунта, с которого приходили письма, были результативными – они были создан для того, чтобы отправить сообщения, а затем заблокированы. Сбор предварительной информации показал, что к инциденту могут быть причастны более тридцати человек. Психологический портрет злоумышленника совпал с профилями двух сотрудников в ProfileCenter. С каждым сотрудником провели опросную беседу. Причастные лица было выявлены.

– откаты, подработки, боковики и др. по делам об экстремизме и терроризме в информационной сфере (корыстный мотив). *Инструментами для выявления значимой информации (инструментами для мониторинга) явились следующие:* выявляли информацию на тематику, например, «тендор, награда, интерес, внимание» – поиск по синонимам. При определенном контексте эти слова воспринимались как синонимы. При исследовании синонимов важна комбинаторика, количество вариаций и порядок, количество нейтральных слов между ними, пе-

ресечение множеств, контекст: местоимение (я, мы, твой, ваш) и значимый стимул (глагол-действие). В основном, в переписке использовали местоимения.

В завершении, по результатам исследования практик киберинцидентов, важно отметить следующее:

– мотивами инсайдеров явились корыстный и (или) идеологический. Инсайдерские атаки по идеологии субъективны и иррациональны. Их сложнее просчитать. Однако их контроль осуществлялся теми же инструментами и программными продуктами, что и корыстный мотив. Использование программных продуктов при выявлении корыстных мотивов использовать гораздо проще: есть возможность четко формализовывать отдельные процессы.

– характеристика и значимые признаки социальной инженерии важны как для личной безопасности, так и для корпоративной безопасности. Необходимо знать, как атакуют злоумышленники, например, фишинг – это сообщение, которое побуждает к действию получателя письма по ссылке. По результатам исследования инсайдеры успешно реализовали атаки, используя социальную инженерию или обратную социальную инженерию (создавали условия, чтоб жертва сама принимала инсайдера за доверенное лицо. Не инсайдера инициировал обращение к жертве, а наоборот.

– атаки инсайдеров значительно влияли на дальнейшую жизнь и привычки пострадавших.

– анализ практических исследований показал, что предпринимаемые меры по предупреждению инсайдерских угроз носят блочный характер, направлены на нейтрализацию отдельных угроз. Современные цифровые атаки связаны с действиями людей, их психологией поведения, шаблонными инструментами воздействия на пользователей.

В этой связи, мы полагаем, что эффективное противодействие цифровым атакам базируется на следующих системных алгоритмах [1]:

– анализа исследования закономерностей (характеристик) цифровых атак: важно выявить их информативные особенности (маркеры), в том числе отрабатывая психологию поведения злоумышленника, его уязвимости;

– реагирования на цифровые атаки – необходимо обучение пользователей предупреждению, распознаванию атак, их своевременной фиксации (сохранению цифровых следов);

– оперативного взаимодействия пользователей при выявлении цифровых атак с правоохранительными органами;

– оперативного взаимодействия правоохранительных органов (в том числе международных, межведомственных, внутриведомственных) с кредитными организациями, операторами сотовой связи, специалистами и др.

Использование вышеуказанных алгоритмов при комплексном подходе к защите от инсайдерских угроз повысит эффективность их контроля и предупреждения, в том числе, по делам о преступлениях об экстремизме и терроризме в информационной сфере.

Список литературы

1. Лонщакова А. Р. Системные механизмы противодействия использованию криптовалют и электронных средств платежа в сфере незаконного оборота наркотических средств, психотропных веществ и их аналогов// Евразийский юридический журнал. 2021. № 6. С. 365–367.

2. Поезжалов В. Б., Линкевич А. Е. Разъяснения Пленума Верховного Суда Российской Федерации: спорные вопросы судебного толкования // Евразийская адвокатура. 2016. № 5 (24). С. 21–24.

3. Харисова З. И., Лонщакова А. Р. Программно-аналитический комплекс «Кибербезопасность» // Свидетельство о регистрации программы для ЭВМ 2020661720, 30.09.2020. Заявка № 2020660996 от 23.09.2020.

Клочкова Е. Н.[1]***,***
доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

МЕТОДИКА ВЫЯВЛЕНИЯ ПРИЗНАКОВ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ИДЕОЛОГИИ В СЕТИ ИНТЕРНЕТ

Бурное развитие информационных технологий, цифровизация общества приводит к тому, что все больше людей ежедневно используют ресурсы сети Интернет. В настоящее время масштабы использования сети таковы, что Интернет необходимо относить к средствам массовой информации. Наиболее активными пользователями сети в первую очередь является молодое поколение, которые родилось, выросло в период появления и стремительного развития цифровой культуры. Они привыкли фактически с рождения использовать различные электронные ресурсы для общения, развлечения, поиска и передачи информации. Молодежь привыкла к тому, что, если им что-то необходимо, то это обязательно есть в сети Интернет, зачастую слепо доверяя тому, что там прочитали. Молодое поколение уже фактически не использует никаких других источников информации, не читает печатных книг, газет, журналов, не смотрит телевизор. Сеть Интернет стала для них основным, фактически единственным каналом получения информации.

При этом необходимо отметить, что сеть Интернет не является безопасной средой. Наряду с традиционной, «полезной» информацией, там находит отражение и противоправный контент экстремистской, террористической и т. д. направленности. Различные представители экстремистских движений уже давно поняли перспективы использования сети Интернет для продвижения своей идеологии. Наряду с сайтами, которые носят откровенно террористический, экстремистский характер, в сети функционирует значительное количество ресурсов, которые напрямую не имеют никакого отношения к террористическим организациям, но при этом могут оказывать им поддержку в различных формах. Если первые выявить достаточно просто и заблокировать к ним доступ, то со второй категорией работать значительно сложнее. Специфика организации работы в сети заключается еще и в том, что в случае блокирования доступа к одному из сайтов, он может просто сменить свой адрес, сервер регистрации.

В настоящее время террористические организации сильно изменились, имея достаточное финансирование, они в своей деятельности могут использовать самые современные достижения, привлекать высококвалифицированных специалистов. Так разработкой сайтов занимаются IT-специалисты, которые разбираются не только в том, как создать страницу в сети, но и прекрасно понимающих как привлечь внимание именно к ней, заставить пользователя прочитать ее, ознакомиться с ее содержанием. Создаваемые сайты обычно отличаются привлекательностью инфографики, оперативностью обновления информации, быстрым откликом на происходящие события, адресной ориентацией на самые

разные категории пользователей. Для привлечения молодежи, например, создаются страницы, там, где подростки больше всего проводят времени, т.е. в различных социальных сетях. Ориентируясь на конкретную социальную группу, меняется стиль подачи материалов, используемая лексика.

Молодежь является наиболее уязвимой категорией общества. Это связано, прежде всего, с тем, что подростки зачастую еще не имеют полностью сформированного взгляда на мир, отсутствует критический взгляд на информацию. Неумение анализировать обычно служит хорошим фоном для сообщений, игр о «хороших» террористах, смертников и т.д., которые постепенно меняют мировоззрение пользователя. При этом для поощрения, поддержания интереса используются различные виртуальные деньги, очки, которые необходимо собирать. Очень часто для получения такого виртуального одобрения молодой человек готов пойти на поступки, которые в обычное время он бы не совершил.

Для продвижения своей идеологии террористические и экстремистские организации используют самые разнообразные способы подачи материалов, это могут быть сообщения, аудиофайлы, фильмы, книги, статьи, специально разработанные игры. Отличительной особенностью таких материалов становится их радикальный, субъективный характер, в которых часто фигурируют такие ключевые слова, как насилие, агрессия. Агрессия может быть направлена как другого человека, так и на общество в целом.

Понимая опасность распространения экстремистской и террористической идеологии в сети Интернет, а также ее губительное влияние на подрастающее поколение правоохранительные органы ведут активную работу по выявлению и блокированию такого противоправного контента. Для упрощения поиска экстремистского и террористического контента по ключевым словам разработан специальный словарь лингвистических маркеров, в который были включены специфические термины и словосочетания.

Если общедоступный контент в сети, открытые группы в социальных сетях фактически исчезли, то скрытых групп еще более чем достаточно, многие из них переместились в закрытые беседы и чаты, продолжая вовлекать молодежь в противоправные деяния.

Определим признаки, по которым можно выявить, что пользователь социальной сети заинтересовался террористической идеологией. Страница в социальной сети в настоящее время может стать отличным индикатором такой вовлеченности. Рассмотрим отличия таких страниц от страниц обычных пользователей.

Социальные сети изначально предназначены для общения и поиска друзей, поэтому профиль обычного пользователя содержит все достаточное количество правдивой информации о владельце: интересы, фотографии и т. д. Каждый пользователь имеет определенное количество подписок, которые отражают его интересы.

Для пользователя, подверженного воздействию террористической агитации, характерно изменение профили, сокрытие информации о себе и изменение характера подписок. В большинстве случаев они будут либо на паблики, распространяющие материалы экстремистской, террористической направленности,

либо на уже заблокированные Роскомнадзором, либо «резервные» паблики. Список друзей часто тоже меняется, среди них могут оказаться те, кто публикует противоправные материалы. Появляются посты, содержащие видео-, фотоматериалы с мест боевых действий, фотографии с изображением казни заложников, с оружием, информацию по изготовлению взрывных устройств, способам противодействия правоохранительным органам и т. д. Еще одним признаком может стать наличие репостов материалов с уже заблокированных аккаунтов. При этом могут быть и косвенные признаки, говорящие о вовлеченности пользователя в противоправную деятельности, такие как неоправданно большое количество просмотров постов при минимуме подписчиков, наличие запасных и резервных групп и ссылок на них, минимум репостов и лайков.

Возможен другой вариант, когда на странице нет прямых признаков экстремистской и террористической идеологии, но в тоже время пользователь стал интересоваться пабликами о несправедливости существующего государственного устройства, о противоправных действиях сотрудников правоохранительных органов в отношении определенной категории граждан и т. д. При этом пользователь отписывается от всех других пабликов, которые были у него раньше.

В заключении хотелось бы отметить, что нами были рассмотрены только некоторые из признаков, по которым происходит выявление пользователей, подверженных воздействию террористической агитации. И здесь необходимо помнить, что после обнаружения пользователя сразу возникает другая проблема, связанная с его идентификацией, когда необходимо соединить виртуальный мир и реальный. И принимать меры требуется уже в реальном мире, к реальному человеку. Но в тоже время нельзя не отметить, что мониторинг сети Интернет является важнейшим элементом общегосударственной работы по защите информационного пространства от проникновения и распространения деструктивных идей, в том числе экстремистской и террористической направленности.

Список литературы

1. Профилактика экстремизма и террористического поведения молодежи в интернет-пространстве: традиционные и инновационные формы : методическое пособие // URL: https://www.nstu.ru/static_files/63706/Prevention.pdf (дата обращения: 11.11.2021).

2. Методические рекомендации по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации / под ред. В. В. Попова // URL: https://losinka.mos.ru/housing-and-communal-complex/information/ Профилактика % 20терроризма%20в%20соц%20сетях.pdf (дата обращения: 11.11.2021).

3. Методические рекомендации по противодействию идеологии экстремизма и терроризма в сети Интернет // URL: https://ksu.edu.ru/files/Svedeniya_ob_organisacii/ANTITERROR/antiterror-mr-v-seti-internet.pdf (дата обращения: 11.11.2021).

Пакляченко М. Ю.[1]**,**
старший преподаватель
кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

О СОДЕРЖАНИИ ИНСТРУКТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стандартизация в области информационной безопасности предполагает под собой осуществление деятельности по разработке и введению в действие, применению документации, в которой определены правила, характеристики, техники, технологии и подходы, методы и алгоритмы, коррелирующие с разнообразными направлениями в сфере защиты информации, в том числе в различных областях, требующих для соответствующих данных (сведений, сообщений) обеспечения безопасности.

Функциональный состав данного рода инструктивных документов формируется из следующего:

– формирование единого терминологического аппарата в области информационной безопасности и защиты информации (ИБ и ЗИ, соответственно);

– создание системы измерений определения уровня и соответствующих критериев ИБ и ЗИ, их конкретизация и топологизация;

– согласование и единообразие оценки качества и эффективности компонентов систем ЗИ;

– популяризация лучших практик, формализация наиболее эффективных подходов к обеспечению ИБ и ЗИ;

– нормотворчество (в части приобретения стандартами юридической силы и установления условий и требований обязательного соответствия им).

В сфере регулирования информационных правоотношений указанные инструктивные документы рационально классифицировать по прикладному и процессорному критерию. В рамках такой дифференциации можно выделить две группы стандартов:

– контрольно-технические, регулирующие вопросы прикладной реализации мер обеспечения безопасности информации, а также их оценки;

– процессно-ориентированные, курирующие аспекты в части определения состава процедур и их последовательного (или параллельного) исполнения, разработки архитектур систем информационной безопасности.

Потребность в защите персональных данных (далее – ПД) и соответствующей многоуровневой (по юридической силе) и многоаспектной (адресность, тип обработки: автоматизированная/неавтоматизированная, категория ПД) регламентации процессов их обработки, стремительно возрастает ввиду массовости и повсеместности работы с ПД, а также по причине цифровизации обще-

ства и государства. Отрадно, что в данном направлении ведется динамичная деятельность по установке правил обработки данного вида информации, требующей соблюдения режима конфиденциальности ввиду своей значимости для различных участников информационных правоотношений.

Ключевая регламентация обработки ПД и обеспечения их защиты осуществляется советующим Федеральным законом [1] (далее – 152-ФЗ, закон о ПД). Приоритетным направлением реализации документа выступает защита свобод и прав граждан путем качественного обрабатывания их ПД, он также определяет принципы и условия обработки (использования) ПД, главных участников информационных отношений и их правовой статус, категории ПД, раскрывает меры по обеспечению безопасности данных, устанавливает регуляторов и ответственность за нарушение требований закона.

Как подтверждает практика, наличия и нормативных документов подобного уровня очевидно недостаточно. Конкретизация законодательно обозначенных аспектов работы с ПД находит свое отражение в источниках, издаваемых Правительством Российской Федерации [2] и регуляторами [3, 4], а также в системе стандартов по соответствующему направлению [5, 6].

В данной статье будет рассмотрено содержание ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных» (далее – ГОСТ, стандарт) и выполнен его концептуально-семантический анализ в контексте соответствия, дополнения и конкретизации положений федерального законодательства.

Стандарт представляет описание архитектуры (перечень компонентов) информационных систем обработки ПД (ИСПД), мер защиты информации в данных системах на базе высокоуровневого подхода к их реализации, технологии, обеспечивающие конфиденциальность ПД, которые могут также использоваться как меры защиты.

В разделе 3 настоящего ГОСТ приведены термины и определения, которые в большинстве заимствованы из 152-ФЗ, однако некоторые из них достаточно коллизионны относительно базового закона о ПД. В частности, в определении безопасности ПД, как «состояния защищенности таких данных, характеризуемого способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПД при их обработке в ИСПД», отсутствует упоминание об операторе, важнейшем субъекте советующих информационных отношений по обработке ПД и определении ее целей.

В примечании к терминологии, используемой в ГОСТ, указано среди прочего, что «ПД являются, например, … семейное, социальное, имущественное положение, образование, профессия, доходы …». На наш взгляд само «положение» или «профессия», не могут по своему существу являться ПД, корректнее было бы употребить термин «сведения о» положении, профессии и т.д. Ст. 7 152-ФЗ находит свое отражение в стандарте в форме дефиниции конфиденциальности ПД, также введено понятие нарушителя безопасности ПД и угроз безопасности ПД. На наш взгляд, данные определения было бы целесообразно включить в ст. 3 закона о ПД.

Следующий раздел анализируемого ГОСТ приводит общий обзор базовой архитектуры защиты ПД, которая предназначена для использования в качестве технического руководства для разработчиков ИСПД. Архитектура представляется набором уровней, состоящих из сгруппированных компонентов, имеющих общую цель или сходную функцию. Она также разделена на части относительно участников обработки ПД. За ней следует модель реализации, определяющая архитектуру с точки зрения автономной ИСПД, затем – представления архитектуры с точки зрения взаимодействия.

Кроме этого базовая архитектура представляет правила соответствия между так называемыми значимыми вопросами, отражающими необходимость обеспечения ПД, и точками зрения посредством таблиц соответствия. Перечень примеров значимых вопросов приведен в приложении к стандарту, где они разбиты на группы подвопросов относительно уровней системы. Среди уровней отмечаются: представление с точки зрения компонентов, представление с точки зрения субъектов, представления с точки зрения взаимодействия, которые соотносятся с этапами жизненного цикла ПД при обработке (сбор, передача, использование, хранение).

Интересен ряд требований, содержащихся в раскрытии определенных этапов жизненного цикла ПД при обработке. Так, для этапа «Использование» стандартом установлено обязательство в части предоставления для субъекта ПД способа связи с оператором ПД в случае возникновения любых вопросов о каких-либо действиях, которые ему не ясны. На наш взгляд данное положение также гармонично бы дополнило содержание действующего закона. Вместе с этим целесообразно включить позиции о блокировании ПД, отсутствующие на сегодняшний день в 152-ФЗ. В стандарте под ним понимается архивирование и защиты с помощью механизма управления доступом для предотвращения дальнейшего использования.

Раздел 5 посвящен участникам обработки ПД, среди которых выделяют следующие стороны: субъект ПД, оператор ПД и обработчик ПД, которому оператор ПД поручает обработку. Стоит отметить, что упоминания о последнем из представленных в стандарте участников в 152-ФЗ отсутствуют. Дефиниция обработчика ПД также не приводится в разделе «Термины и определения» ГОСТ.

Особого внимания заслуживает приведения принципов обеспечения безопасности ПД: согласие и выбор, законность цели и ее спецификация, минимизация данных, ограничения в отношении использования, хранения и раскрытия, точность и качество ПД, открытость, прозрачность и уведомление, персонифицированный доступ, ответственность, обеспечение безопасности информации, соответствие требованиям нормативной правовой базы. Указанный перечень в достаточной степени согласуется с законодательно определенными условиями обработки ПД (ст. 5 152-ФЗ).

Отдельно хочется отметить вводимые стандартом графические модели, описывающие меры защиты в ИСПД. Так в частности, говорится необходимости разработки блок-схем обработки ПД, представляемых в виде таблиц потоков ПД. В подобных таблицах отслеживаются процессы сбора, передачи, использования, хранения и уничтожения ПД. Они являются основой формирования мо-

дели угроз и модели нарушителя безопасности ПД. Кроме этого приводятся таблицы взаимосвязи между упомянутыми ранее принципами обеспечения безопасности ПД и компонентами на различных уровнях (установок, управления идентификационными данными и управления доступом, уровне ПД).

На наш взгляд, приведенные в ГОСТ методики и техники, устанавливаемые им категории, являются полезным руководством при разработке ИСПД и реализации мер защиты ПД для организаций, взаимодействующих с данными системами: проектирующих, администрирующих и эксплуатирующих их. Большинство позиций, представленных в данном инструктивном документе, заслуживают быть включенными в содержание источников, обладающих большей юридической силой, в своей сущности не противоречат положениям действующих нормативных правовых актов в области защиты ПД.

Список литературы

1. Федеральный закон Российской Федерации от 27 июня 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/.

2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?=doc&ts=823wVsS5HBaHmuYA&cacheid.

3. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_146520/.

4. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_167862/.

5. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст : введен впервые : дата введения 2014-09-01 // URL: https://docs.cntd.ru/document/1200108858.

6. ГОСТ Р 53647.6-2012. Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по

техническому регулированию и метрологии от 29 ноября 2012 г. № 1421-ст : введен впервые : дата введения 2013-12-01 // URL: https://docs.cntd.-ru/document/1200096844.

Лустин В. И.[1]***,***
старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ТОНКАЯ ГРАНЬ МЕЖДУ БАНДИТИЗМОМ И ТЕРРОРИЗМОМ

Многие из тех, кто устраивает теракты, ранее имели тесную связь с преступными кругами или даже были вовлечены в их деятельность. Более того, доходы от незаконной преступной деятельности являются источником финансирования большей части терактов.

В исследованиях указывается на тонкую грань между преступными и террористическими организациями джихадистской направленности в Европе. Учитывая, данные факторы, можно увидеть тесные связи между преступностью и терроризмом во многих странах. Основываясь на подробном анализе Международного центра исследования радикализации и политического насилия, необходимо отметить тот факт, что ряд вставших на сторону террористических движений джихадистов, проживающих в Европе, находились ранее в преступной среде, а также отбыли наказание за эту деятельность.

Выявленная закономерность прослеживается для многих активных членов в террористической организации. Однако, это работает не для всех категорий джихадистов, некоторые из которых считались хорошо интегрированными и занимающимися честной деятельностью. Женщины, с другой стороны, занимают особое положение и вовлекаются в сотрудничество на религиозной основе.

Рассматривая далее и возвращаясь к мелким преступникам, ставшим джихадистами, отмечается, что террористическим организациям удалось стать привлекательными в достаточной степени, чтобы заставить их уйти из своей обыденной жизни. Более того, их убедили, что им нужно пожертвовать собой на алтарь нового «дела». Вербовщики нелегко предлагали им приключения «Безумного Макса», при этом использовались методы психологического и религиозного и воздействия, предлагалось искупление всех прошлых прегрешений (какими бы они ни были) в джихаде. И это несмотря на то, что руководство террористических организаций, которое по всей территории, еще находившуюся под своим контролем, крайне жестоко наказывает за любые проступки: отрезает руку ворам, забивает камнями за измену и проводит еще более суровые репрессии за другие виды преступлений (например, за употребление и оборот наркотических средств).

Джихадистское движение активно использует квалификацию преступников, отчасти для обеспечения независимости в вопросах финансирования своих ячеек в Европе. Следует отметить, что «Аль-Каида» действовала точно так же: каждая ячейка должна была обеспечить свою деятельность как можно больше.

Насколько тонка здесь линия? «Исламское государство» удивило «Аль-Каиду» и начало вербовать последователей среди «профессиональных» бандитов.

В целом, «Аль-Каида» не казалась особенно привлекательной для европейских преступников. Требовались минимальные знания исламистской идеологии и, часто, для этого необходимо было осуществить следующее: изучить арабский язык в медресе (Египет, Йемен или Пакистан), пройти упорные тренировки в отдаленных лагерях без привычных западных удобств. Фронт в Сирии был новшеством в этом плане, потому что волонтеры находили там не только приключения, но и своеобразное «общество потребления», в котором все и вся переправлялось контрабандой. Одно время его даже называли «джихадистским курортом». Идеологи религиозных террористических движений прекрасно поняли настрой и стремления молодых западных бунтарей. И они дали им то, чего они ждали.

Необходимо отметить, что ИГИЛ по своим собственным причинам установил тесные связи с международными преступными организациями, такими как турецкая мафия. Именно она была занята, то есть поставками людей и оборудования ИГИЛ и получала в обмен нефть, антиквариат и сырье. Однако не удалось выявить в полоном объеме, масштабы незаконного оборота наркотиков, который, по-видимому, используется ИГИЛ. В этой области «Аль-Каида» и ее поставки афганского опиума в различные регионы имеют приоритет.

Дело в том, что такие перемещения требуют от преступности активных действий в логистических целях. Высокопоставленные преступники заинтересованы в получении прибыли от своей деятельности, поэтому сотрудничество организованной преступности и террористических движений осуществляется до тех пор, пока оно приносит доход. Возможно, турецкая мафия потеряет интерес к ДАИШ, так как «Исламское государство», скорее всего, прекратит свое существование как таковое, хотя, не будем питать никаких иллюзий, завтра этого не произойдет. Таким образом, борьба с преступностью может помочь нам в борьбе с терроризмом, лишив его части финансирования.

Новый фактор современности состоит в том, что ДАИШ вербует среди преступников. Если эти активисты не в силах отправиться на землю джихада, то могут начать борьбу в своей стране, воспользовавшись связями в преступных кругах для формирования опасных независимых ячеек.

Как обычно, какого-то одного глобального решения тут не существует. Эффективнее бороться с двумя этими явлениями можно лишь при действительной реализации следующих мер: приведение законов (по возможности) к общему знаменателю, расширение сотрудничества судебных органов, полиции и разведки и т. д. Договариваться об этом можно лишь на самом высоком политическом уровне. И хотя интересы там зачастую расходятся, борьба с преступностью и терроризмом не может не интересовать подавляющее большинство государственных лидеров.

Борьба с террористическими движениями должна проводиться совместно борьбой с организованной преступностью и правонарушениями в целом.

Основными разграничивающими признаками этих преступлений выступают элементы объективной стороны и цели совершения преступлений. Обязательный признак объективной стороны бандитизма – создание устойчивой, вооруженной группировки (банды) в целях нападения. При терроризме создание тер-

рористической группировки – лишь приготовление к квалифицированному терроризму, а террористический акт, совершенный организованной группой – квалифицированный терроризм. Нападение – основное общественно опасное действие бандформирований. Терроризм не связан с насилием над конкретными людьми и представителями государственных и общественных организаций, он, скорее, представляет собой «рассеянную» угрозу или опасность населению, обществу.

Таким образом, бандитизм – это организация устойчивой преступной группы, которая может быть мобилизована в любой момент и преступления направлены в основном против интересов граждан, а терроризм – это преступления против государства с предъявлением неких условий, требований.

Список литературы

1. Глебова Н. Экономика «Исламского государства» // URL: http://rabkor.ru/columns/analysis/2015/07/15/the-isis-economy/.

2. Дамаскин О. В. Криминологические аспекты детерминации современного экстремизма и терроризма : монография. М., 2018. 259 с.

3. Клейменов И. М. Международный терроризм и транснациональная организованная преступность // Вестник Омского университета. 2017. № 3 (52).

4. Тихонов А., Медведев С. Как противостоять терроризму // URL: http://archive.redstar.ru/index.php/eliseeva/item/5018-kak-protivostoyat-terrorizmu.

Михайленко Н. В.[1]*,*
доцент кафедры административной деятельности
органов внутренних дел
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

Мурадян С. В.[2]*,*
старший преподаватель кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА И ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ОДНОРАНГОВЫХ СЕТЕЙ

На сегодняшний день применение одноранговых сетей имеет высокий практический потенциал. Это связано с тем, что они лежат в основе современных блокчейн-систем, прежде всего из-за возможности обмена криптовалютами и цифровыми активами через распределенную сеть, что позволяет осуществлять операции в короткие сроки и без посредников. Преимуществом одноранговых (в отличие от многоранговых или иерархических сетей) выступает фактическое отсутствие единого сервера, обеспечивающего хранение и обработку данных клиентов.

Структура построения и принципы функционирования одноранговых сетей делают их привлекательными не только для успешного применения бизнес-сообществом, но и объектами преступного посягательства при совершении преступлений против собственности. P2P предлагает уникальные преимущества, которые в свою очередь таят в себе уникальные угрозы и риски. Актуальность оптимизации работы по противодействию киберправонарушениям в указанном сегменте подтверждается тем, что России отмечается увеличение атак в 2021 г. на блокчейн-сети на 46 % в сравнении с аналогичным периодом 2020 г.

В последнее время, отмеченные преимущества одноранговых сетей стали активно использоваться террористами и экстремистами для целей надежной передачи данных и в качестве канала финансирования [1].

Прежде всего, действия злоумышленников затрагивают вопросы блокчейн-систем и криптосервисов, основанных на peer-2-peer-взаимодействии.

Можно выделить персональные и технологические аспекты противоправного поведения таких лиц в сети.

К персональным относится использование методов социальной инженерии в отношении пользователей (узлов) системы.

Атаки с применением социальной инженерии нацелены на торгового контрагента. Мошенники используют обман и злоупотребление доверием, чтобы за-

владеть средствами или личными данными. Мошенничество и фишинг – их самые распространенные методы. Злоумышленник выдает себя за настоящего трейдера, заинтересованного в покупке или продаже Биткоина или других криптовалют на P2P-платформе. Он может разместить собственное торговое объявление или ответить на существующее. Альтернативная техника, широко распространенная на централизованных маркетплейсах, – имитация службы поддержки. В этом случае злоумышленник, связавшись с вами, выдает себя за сотрудника торговой платформы и, как правило, пытается получить от вас личную информацию или детали платежа.

На сегодняшний день активно применяются мошеннические схемы при покупках криптовалют, например, биткоина на Binance P2P. Продавец просит отменить сделку после оплаты со стороны покупателя. Если покупатель соглашается, то эскроу-сервис возвращает криптовалюту обратно на кошелек продавца. Продавец просит покупателя осуществить сделку за пределами P2P-платформы, то есть в отсутствии доступа к эскроу-сервису, а значит без гарантий получения криптовалюты после оплаты. И третий из наиболее часто встречающихся, вариант, когда продавец просит оплатить дополнительную комиссию помимо комиссии заявленной маркетплейсом, то есть пытается получить незаконно вознаграждение от покупателя.

Среди мошеннических схем, используемых при продаже криптовалют можно выделить блокировку монет, когда контрагент отмечает сделку как «оплаченную», даже если не отправил платеж. А при попытке связаться с ним, он обычно не отвечает. Эта разновидность мошенничества обычно нацелена на новичков, более склонных к таким ошибкам, ввиду небольшого опыта. Самый банальный способ, когда контрагент просит взаймы с обещанием выплатить долг с высокими процентами. Иногда, покупатель требует перевести монеты до завершения платежа. Такой перевод лишает участника сделки гарантии на отправку средств со стороны покупателя.

Подобные действия квалифицируются по ст. 159 Уголовного кодекса Российской Федерации, как мошенничество. Если же, впоследствии денежные средства, полученные с применением методов социальной инженерии, будут направлены на финансирование терроризма и экстремистской деятельности, тогда потребуется дополнительная квалификация по ч. 1^1 ст. 205^1 и ст. 282^3 Уголовного кодекса Российской Федерации.

Среди технологических выделяются прямые кибер- и скриптинг-атаки. При этом, если современный уровень информационной безопасности позволяет своевременно выявлять прямые кибератаки и успешно противостоять им, то скриптинг представляет собой наиболее вредоносный способ атакующего воздействия, прежде всего из-за возможности сочетания с другими видами атак. Подобные действия будут квалифицированы, в зависимости от особенностей реализации объективной стороны по соответствующим составам преступлений, предусмотренным нормами главы 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации». А, при необходимости, также в совокупности с ч. 1^1 ст. 205^1 и ст. 282^3 Уголовного кодекса Российской Федерации.

Распределенная архитектура делает все P2P-сети относительно устойчивыми к различным кибератакам [2], но наиболее приоритетными по своему функционалу выступают гибридные P2P-сети, обеспечивающие большую безопасность данных от всех форм враждебной активности в сети, прежде всего за счет своей одноранговой структуры.

Однако, все виды одноранговых сетей имеют ряд существенных недостатков. Во-первых, все увеличивающиеся с развитием информационных технологий, риски подверженности атакам, перечисленным выше, а также сравнительно высокие риски аутентификации в сети сторонних лиц.

Надежность таких систем, представляющая собой преимущество, с одной стороны, является их вторым существенным недостатком, с другой. Ряд операций в одноранговых сетях, в том числе и по приобретению средств, планируемых к использованию в целях осуществления финансирования терроризма и экстремизма, может осуществляться при высокой степени анонимности, что существенно осложняет возможности контроля за операциями, происходящими внутри сети со стороны федеральных органов исполнительной власти, делая установление личности преступников, причастных к совершению преступлений с использованием этих сетей, практически недосягаемым результатом для сотрудников правоохранительных органов.

Раскрытие и расследование преступлений, предусмотренных ч. 1^1 ст. 205^1 и ст. 282^3 Уголовного кодекса Российской Федерации, осложняет и тот факт, что некоторые одноранговые сети не позволяют легко определять первичный источник файла, так как, по сути, любой узел в таких сетях, при его востребованности, может выступать посредником при передаче, скрывая истинный источник. Указанное посредничество будет выступать исключительно технической особенностью, не зависящей от воли пользователя, и, соответственно, участие в распространении деструктивного контента пользователей (узлов) сети будет непреднамеренным. В большинстве случаев, пользователи и не знают о процедуре передачи файла другим пользователям. В таком случае установить первичный или оригинальный источник файла не представится возможным.

В практике правоохранительных органов при невозможности установления инициатора, под источником обычно понимается конечный пользователь (узел), использующий файл или код, что является спорным и, зачастую, существенно усложняет производство по уголовным делам.

Для успешного противодействия финансированию терроризма и экстремистских организаций, осуществляемого при использовании P2P-сетей, необходим комплексный мониторинг данных систем со стороны федеральных органов исполнительной власти, с подключением к указанному процессу специалистов правоохранительных органов или иных субъектов, что обусловлено следующими факторами:

– одноранговые сети предоставляют пользователям системы возможность осуществлять взаимодействие в рамках закрытой системы, что предусматривает высокую степень латентности операций, а также полную или частичную анонимность (в связи с чем одноранговые сети очень популярны среди пользователей даркнетat, среди которых определенную часть занимают лица, пресле-

дующие цели сбора средств для осуществления террористической и экстремистской деятельности);

– одноранговые сети служат платформами для осуществления различных категорий сделок между пользователями напрямую без участия посредников, в том числе активно применяются в майнинге, доход от которого может быть направлен на финансирование терроризма и экстремисткой деятельности;

– одноранговые сети, при несоблюдении условий конфиденциальности всеми участниками сети (узлов), являются объектами фишинга и иных видов противоправных действий с минимальными возможностями идентификации личностей злоумышленников;

– в одноранговых сетях отсутствует механизм распознавания участников сети.

Рассмотренные аспекты и необходимость процессуального сопровождения системы противодействия киберугрозам в одноранговых сетях, либо их использования в противоправных целях, показывают, что привлечение органов внутренних дел к общей системе профилактики и мониторинга инцидентов, оценке рисков и цензурированию операций, проводимых в рамках P2P-соединений, является обоснованным и перспективным направлением противодействия финансированию терроризма и экстремистских организаций в свете растущей цифровизации всех сфер жизни общества.

Следует отметить, что на сегодняшний день отсутствует единая система классификации инцидентов в области информационной безопасности [3], в том числе, и в контексте применения возможностей P2P-сетей и платформ, основанных на одноранговых сетях.

На основании изложенного следует рассмотреть ряд предложений, направленных на оптимизацию системы мониторинга функционала одноранговых сетей и деятельности органов внутренних дел:

– передать органам внутренних дел ряд административно-юрисдикционных полномочий по предупреждению и пресечению правонарушений в информационно-техническом секторе, предусмотренных гл. 13 КоАП РФ;

– внести изменения в нормативные правовые акты Российской Федерации, в том числе, в Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» официально позволяющие признавать цифровые валюты имуществом в рамках гражданского и уголовного судопроизводства;

– автоматизировать контроль соответствия выполнения требований законодательства, отраслевых нормативных документов и международных стандартов пользователями одноранговых сетей;

– проработать единую модель классификации инцидентов, возникающих в процессе использования одноранговых сетей, в соответствии с государственным стандартом по обеспечению информационной безопасности и действующим федеральным законодательством в области защиты информации;

– предоставить представителями банковского и кредитного сектора органам внутренних дел дополнительных возможностей по участию в совместной

реализации направлений политики информационной безопасности в финансовой и кредитно-денежной сфере;

– проработать совместные пути по внедрению российской платформы мастерчейн и «цифрового профиля» при осуществлении дистанционных операций с цифровыми финансовыми активами.

Список литературы

1. Мурадян С. В. Актуальные проблемы противодействию финансированию терроризма с использованием криптовалюты. // Актуальные проблемы международного сотрудничества в борьбе с преступностью : сборник статей по итогам Международной научно-практической конференции, приуроченной к 20-летию принятия Конвенции ООН против транснациональной организованной преступности, 29 октября 2020 г. М. : Московский университет МВД России имени В.Я. Кикотя, 2020. С. 110–118.

2. Одноранговые сети. // Binance Academy. URL: https://academy.binance.-com/ru/articles/peer-to-peer-networks-explained (дата обращения: 14.11.2021).

3. Михайленко Н. В. Цифровое государственное управление. Современные проблемы и перспективы завтрашнего дня // Государственная служба и кадры, 2020. № 2. С. 171–175.

4. Мурадян С. В. Факторы, обусловливающие рост числа преступлений, совершаемых с использованием криптовалют и способы их нивелирования в России // Актуальные вопросы современной криминологической и уголовно-исполнительной науки : сборник тезисов Международной научно-практической заочной конференции памяти доктора исторических наук, профессора А. В. Шаркова, 15 апреля 2021 г. Минск : Академия МВД, 2021. С. 208–210.

5. Официальный сайт Национального центра информационного противодействия терроризму и экстремизму // URL: https://ncpti.su/profilakticheskie-materialy/ (дата обращения: 30.10.2021).

Вихляев А. А.[1]**,**
преподаватель кафедры
административной деятельности органов внутренних дел
Московского университета МВД России имени В.Я. Кикотя

НЕКОТОРЫЕ ПРОБЛЕМЫ ОПТИМИЗАЦИИ СИСТЕМЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБМЕНА ДАННЫМИ В РАМКАХ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ НАЦИОНАЛЬНОЙ ПОЛИТИКИ ПРИ ОСУЩЕСТВЛЕНИИ МОНИТОРИНГА И ПРЕВЕНЦИИ МЕЖКОНФЕССИОНАЛЬНОЙ И МЕЖЭТНИЧЕСКОЙ НАПРЯЖЕННОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Вопросы национальностей продолжают оставаться одними из наиболее актуальных в современном мире. Массовые процессы миграции населения и растущие темпы глобализации оказывают непосредственное влияние не только на социально-экономические сферы жизни, но и затрагивают наиболее глубокие вопросы современного общества: вопросы религии, самоопределения народов, межэтнического и субэтнического взаимодействия, языкового и этнографического разнообразия.

Указанные направления образуют в своей совокупности основные приоритеты действующей национальной политики Российской Федерации.

В свою очередь, базовой стратегией, утвержденной указом Президента Российской Федерации от 19 декабря 2013 г. № 1666 [1], определяются и проблемы, тесно связанные с реализацией основных направлений национальной политики на текущем этапе.

В числе наиболее актуальных для Российской Федерации проблем следует выделить следующие:

– распространение международного терроризма и экстремизма, радикальных идей, основанных на национальной и религиозной исключительности;

– возникновение очагов межнациональной и религиозной розни, которые являются следствием пропаганды экстремистской идеологии;

– незаконная миграция, активное формирование анклавов, пропагандирующих исключительность отдельных этнических групп и идеологий;

– имеющиеся проблемы в реализации и поддержке системы социальной и культурной адаптации иностранных граждан в Российской Федерации и их интеграции в российское общество;

– социальное и имущественное неравенство населения, сложности в обеспечении равных возможностей для социального продвижения и доступа к важнейшим общественным благам, региональная экономическая и технологическая дифференциация;

– частичная утрата этнокультурного наследия, размывание традиционных российских духовно-нравственных ценностей, в том числе вследствие глобализации;

– непреодоленные последствия межэтнических или территориальных конфликтов и противоречий на этнической почве в отдельных субъектах Российской Федерации.

В соответствии с данными официальной статистики [2] за 2018–2020 гг. отмечается высокий процент правонарушений, совершаемых иностранными гражданами и лицами без гражданства, в том числе и по мотивам расовой и религиозной неприязни.

Так, если 2018 г. к уголовной ответственности за совершение преступлений различной степени тяжести было привлечено 32 728 иностранных граждан и лиц без гражданства, что составляет 3,6 % от общего количества преступлений, совершенных гражданами Российской Федерации, то в 2019 и 2020 гг. указанные показатели составили 29 922 (3,5 %) и 29 222 (3,5 %) соответственно. Наибольшее число противоправных действий приходятся на Центральный и Северо-Западный федеральные округа, при этом наиболее криминогенной с позиции преступлений, совершаемых мигрантами, продолжает оставаться Москва: в 2018 г. указанный показатель составил 17 % от общего числа преступлений, совершенных иностранными гражданами и лицами без гражданства на территории Российской Федерации, в 2019 и 2020 гг. – 16,7 % и 19 % соответственно.

Так, в докладе, представленном Московским бюро по правам человека, только за 5 месяцев 2021 г. на территории Российской Федерации было установлен резкий рост преступлений на почве расовой и конфессиональной нетерпимости – превышающий на 45 % показатели предыдущего года.

По данным официальной статистики в 2020 г. имели место 7 нападений на почве расовой и религиозной неприязни, когда, как только за январь–август 2021 г. их зафиксировано 17. Число пострадавших в результате актов агрессии также выросло: 8 пострадавших в 2020 г. и 19 пострадавших лиц – в январе–августе 2021 г.

Одной из отличительных особенностей текущей ситуации в сфере националистического и религиозного экстремизма отмечается безусловный рост числа массовых силовых конфликтов, среди которых можно выделить конфликты, основанные на межконфессиональной и межнациональной розни.

География нападений в связи с проявлениями ксенофобии за январь–декабрь 2021 г. охватывала 5 субъектов Российской Федерации, среди которых Новосибирская область – 1 (1 пострадавший), Москва – 7 (9 пострадавших), Нижегородская область – 1 (2 пострадавших), Санкт-Петербург – 5 (1 убит, 3 пострадавших), Тульская область – 2 (2 пострадавших).

Кроме того, за первые 9 месяцев 2021 г. были зафиксированы массовые силовые конфликты между представителями разных этнических групп в Москве (4), Ленинградской области (1), Санкт-Петербурге (1) и Симферополе (1).

«В условиях пандемии значительную угрозу сохраняют акты экстремизма... Поэтому просил бы коллег и далее решительно бороться с пропагандой нацио-

нализма, ксенофобии и насилия. Хотя квалификация таких преступлений – это очевидно абсолютно – достаточно сложная», – отметил в своем выступлении 30 июня 2021 г. заместитель председателя Совета безопасности Д. Медведев. [3]

Действительно, правонарушения, совершаемые на почве расовой и конфессиональной неприязни, продолжают оставаться одними из самых латентных.

Не менее важным аспектом, влияющим на развитие идеологии межэтнического и межконфессионального экстремизма, остается медийная сфера. В информационно-телекоммуникационных сетях продолжает распространяться контент, основанный на вопросах этнической определенности и дискриминации, расовой и религиозной неприязни, растет и мигрантофобия, активно подогреваемая средствами массовой информации, прежде всего, в сети Интернет.

Безусловно, имеющееся программное обеспечение, по типу «контент-фильтра» позволяет ограничивать доступ к ресурсам экстремистского и деструктивного содержания, однако, следует отметить, что указанное ПО базируется больше на выявлении текстово-контекстного содержания, позволяя блокировать нежелательный контент до его поступления к пользователям, в то время, как открытым остается вопрос мониторинга видеоконтента, который может содержать сведения расовой и этнической дискриминации, пропаганды религиозного экстремизма.

Так, в рамках акции [4], проведенной Национальным центром информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет в 2020 г., в сервисе «ВКонтакте» было выявлено более 160 гиперссылок, содержащих сведения экстремистского характера, среди которых 67 % склоняющих к ненависти по расовым, национальным, религиозным и социальным признакам; 14 % – визуализаций запрещенной экстремистской и националистической символики, 19 % – материалов, находящихся в списке запрещенных.

В настоящее время в соответствии с положениями Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и п. 7 Положения о Министерстве юстиции Российской Федерации функции по ведению, опубликованию и размещению федерального списка экстремистских материалов возлагаются на Минюст России.

В соответствии с инициативой Правительства Российской Федерации был проработан законопроект № 1129469-7, предусматривающий создание специализированного информационного банка данных экстремистских материалов, оператором которого, ответственным за его формирование и ведение, предлагается сделать также Министерство юстиции Российской Федерации.

«Создание банка данных имеет целью обеспечение оперативно-розыскных мероприятий и следственных действий, проводимых в рамках противодействия экстремистской деятельности, и организацию профилактических мероприятий, направленных на ее предупреждение», – изложено в пояснительной записке к законопроекту.

Безусловно, создание единого информационного пространства, которое может позволить своевременно получать данные по различному контенту экстремистского характера позволит своевременно координировать силы и средства

правоохранительных органов по предупреждению правонарушений в сфере религиозного и этнического экстремизма.

Другим перспективным средством мониторинга межконфессиональной и межэтнической напряженности является Государственная информационная система (далее – Система) мониторинга в сфере межнациональных и межконфессиональных отношений и раннего предупреждения конфликтных ситуаций.

Оператором Системы выступает Федеральное агентство по делам национальностей. Введение Системы осуществляется в соответствии с государственной подпрограммой 7 «Профилактика экстремизма на национальной и религиозной почве» Государственной программы «Реализация государственной национальной политики», утвержденной постановлением Правительства Российской Федерации от 29 декабря 2016 г. № 1532, в период с 2017 по 2025 гг.

Указанная Система позволит осуществлять непосредственный мониторинг конфликтных ситуаций межконфессионального и межэтнического характера в информационно-телекоммуникационной сети Интернет (включая средства массовой информации, блоги и социальные сети, экспертные оценки, данные социологических и пр. исследований, посвященных этнопроблематике), осуществлять сбор, обработку, оценку данных о событиях, связанных с проявлениями ксенофобии и религиозной нетерпимостью.

На базе данных мониторинга Система позволит осуществлять анализ и строить прогнозы возникновения конфликтов на национальной и религиозной почве.

Кроме того, инновационным выглядит и реализация возможностей выявления конфликтных и предконфликтных ситуаций, в конфликтующих группах которых усматривается разделение по этническому и (или) конфессиональному признаку, а также в случаях, когда стороны конфликта ищут поддержки в этнически (конфессионально) родственной или этнически (конфессионально) дружественной среде.

Данные мониторинга и аналитические материалы позволят своевременно оповещать о возникновении конфликтов на почве религиозной и националистической неприязни, осуществлять поддержку принятия обоснованных управленческих решений в области государственной национальной политики, производить оценку субъектов Российской Федерации по интегральному уровню конфликтности и социально-экономическим показателям.

В свою очередь, сведения, получаемые в результате указанного мониторинга, позволят сформировать представления об оперативной обстановке, осуществить координацию сил и средств, своевременно планировать и реализовывать комплексные оперативно-профилактические операции, выявлять и пресекать любые проявления межконфессионального и межэтнического экстремизма на ранних стадиях.

В соответствии с проведенным исследованием необходимо сделать ряд заключений.

Националистический и религиозный виды экстремизма продолжают оставаться одними из наиболее глобальных проблем, затрагивающих вопросы национальной безопасности Российской Федерации. На текущем этапе в систе-

ме мониторинга и противодействия межконфессиональному и религиозному экстремизму задействован широкий спектр федеральных органов исполнительной власти, общественных объединений правоохранительной направленности и представителей гражданского общества.

Пропаганда расовой, национальной и религиозной нетерпимости осуществляется не только посредством распространения специальной литературы, но и в следствие применения медиатехнологий, что создает дополнительные вызовы современной правоохранительной системе в области мониторинга и противодействия противоправному поведению.

Формирование и ведение комплексных специализированных банков данных и систем мониторинга конфликтных и предконфликтных ситуаций на почве ксенофобии и религиозных разногласий является важным структурным элементом в общей системе профилактики экстремизма на территории Российской Федерации.

В свою очередь, интеграция указанных сведений в регистры, компилирующие сведения о различных проявлениях противоправного поведения, позволят правоохранительным органам своевременно использовать информационно-аналитические материалы и базы данных для противодействия любым проявлениям межконфессионального и межэтнического экстремизма.

Список литературы

1. Указ Президента Российской Федерации от 19 декабря 2012 г. № 1666 «О Стратегии государственной национальной политики Российской Федерации на период до 2025 года» // URL: https://www.mrech.ru/upload/file/ekonom/strategi.pdf.

2. Официальный сайт Генеральной прокуратуры Российской Федерации. Раздел «Правовая статистика» // URL: http://crimestat.ru/social_portrait (дата обращения: 30.10.2020).

3. Медведев призвал бороться с экстремизмом. Официальный сайт Агентства РИА-новости // URL: https://ria.ru/20210630/medvedev-17392-69815.html (дата обращения: 30.10.2020).

4. Официальный сайт Национального центра информационного противодействия терроризму и экстремизму // URL: https://ncpti.su/profilakticheskie-materialy/ (дата обращения 30.10.2020).

Сабитов Р. Р.[1]**,**
эксперт отдела расследования компьютерных инцидентов
Лаборатории Касперского

ЦИФРОВЫЕ СВИДЕТЕЛЬСТВА ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Рост информационных технологий как на территории Российской Федерации, так и во всем мире, обусловил не только быстрое развитие и эффективное применение информационных сетей (например, увеличил масштабы предпринимательской деятельности; повысил качество и удобство коммуникаций между людьми при прохождении дистанционного обучения и т. д.), но и обеспечил появление новых угроз со стороны киберпреступников.

Анонимность пользователей в информационной среде является почвой, которую используют киберпреступники для достижения своего преступного результата. Здесь необходимо отметить, что информационно-телекоммуникационные технологии в настоящее время внедряются во все сферы общественных отношений стремительными шагами, а законодательные и правоохранительные органы не успевают за таким быстротечным развитием.

В 2020 г. в связи с вспышкой COVID-19 все государства перешли на дистанционный формат обучения и работы, а информационное пространство стало пополняться разным развлекательным и учебным контентном, что позволило киберпреступникам совершать еще большее количество злодеяний, остававшись не пойманными. Рассматривая статистические показатели киберпреступности, можно отметить, что ее уровень достиг 461 тыс. преступлений (цифра не окончательная, так как большое количество преступлений имеют латентный характер) [1].

Проблема киберпреступности заключается в том, что, во-первых, киберпространство постоянно пополняется новыми видами преступлений, новыми способами совершения уже имеющихся видов преступлений. Во-вторых, в информационном пространстве постоянно совершаются уже криминализированные в УК РФ преступления, такие как хищения денежных средств, торговля наркотическими и психотропными веществами, торговля оружием и неправомерный доступ к конфиденциальным данным как рядовых граждан, так и государственных корпораций.

Рассмотрим наглядно некоторые особенности получения цифровых доказательств, которые легко уничтожить и еще легче заблокировать к ним доступ. Однако к методам противодействия можно отнести: шифрование; загрузку с внешнего носителя (или по сети); «ловушки» – электромагниные пушки, кнопки, триггеры и т. д.; пароль под принуждением «двойное дно»; «пыль в глаза».

Рис. 1. Сравнение цифровых и вещественных доказательств

Надо заметить, что специалист по кибербезопасности занимается поиском угроз для цифровой безопасности, их изъятием и фиксацией следов. Между тем специалист должен обладать рядом навыков для выявления скрытых источников кибератак, понимать принципы их осуществления, уметь читать код и оперативно их «переводить», знать методы анонимизации в сети Интернет (например, использование виртуальных частных сетей (VPN), TOR, прокси (http-proxy, socks) и др. серверов-посредников).

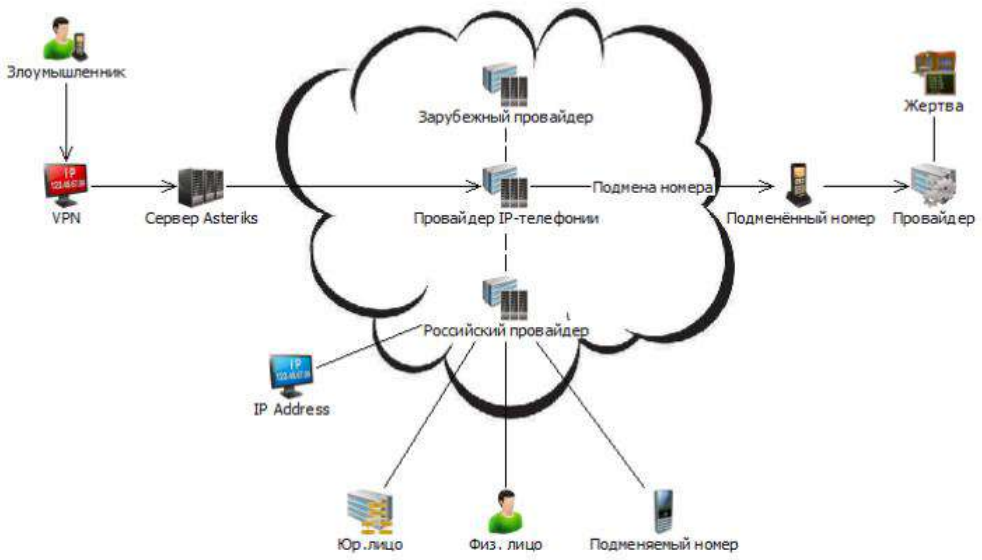


Рис. 2. Схема анонимизации с использованием IP-телефонии

Между тем, специалист по кибербезопасности должен постоянно следить за злоумышленниками в даркнете – скрытая сеть к которой относятся сайты с зашифрованной незаконной информацией, вход в них осуществляется посредством луковых маршрутизаторов. Они отслеживают частные сообщения на веб-серверах, сайтах незаконного оборота наркотиков и анализируют потоки пользователей и данных в «теневом» интернете.

Рис. 3. Составные компоненты поддельного сайта

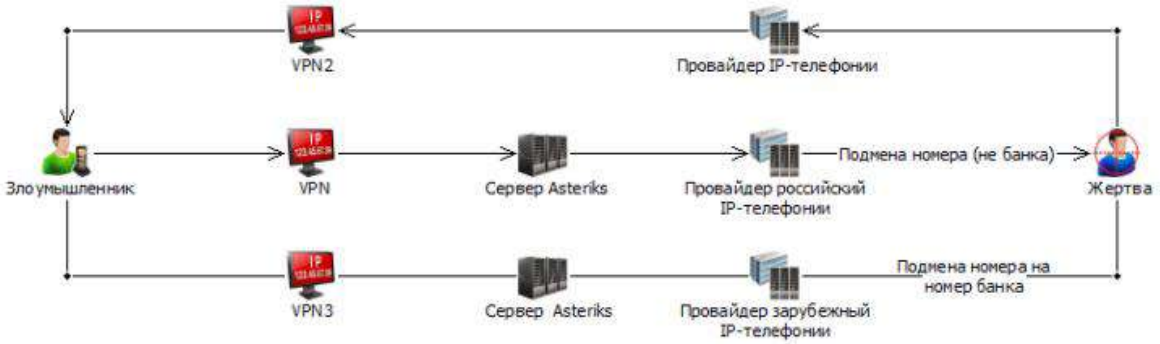


Рис. 4. Схема мошенничества с использованием IP-телефонии, направленная на владельцев банковских карт. Две нити анонимизации – для входящих и исходящих вызовов с подменой номера исходящего звонка

В типовых ситуациях расследования мошенничества, совершенных в даркнете специалист может запрашивать сведения о контактных данных владельца компьютерных устройств, так специалист сможет определить цифровые следы мошенничества, порядок действий при поиске следов приведен на рис. 5.

Поиск следов. Что запрашивать?

Запрос регистратору доменных имен

- Контактная информация (на кого зарегистрирован (ФИО, паспортные данные), когда, с какого ip-адреса регистрировали, контакты (телефон, адрес электронной почты, и т.д.)
- Оплата: список платежей (способ, время, кошельки, и т.д.)

Информация по биллингу

- Контактная информация (на кого зарегистрирован (ФИО, паспортные данные), когда, с какого ip-адреса регистрировали, контакты (телефон, адрес электронной почты, и т.д.)
- Оплата: список платежей (способ, время, кошельки, и т.д.)
- Тип сервера (Виртуальный (VDS/VPS), выделенный (Dedicated) или общий хостинг (Shared hosting), работает ли в настоящий момент
- История заходов в личный кабинет (ip-адреса, время)
- Какие сервера (услуги) еще брал указанный клиент

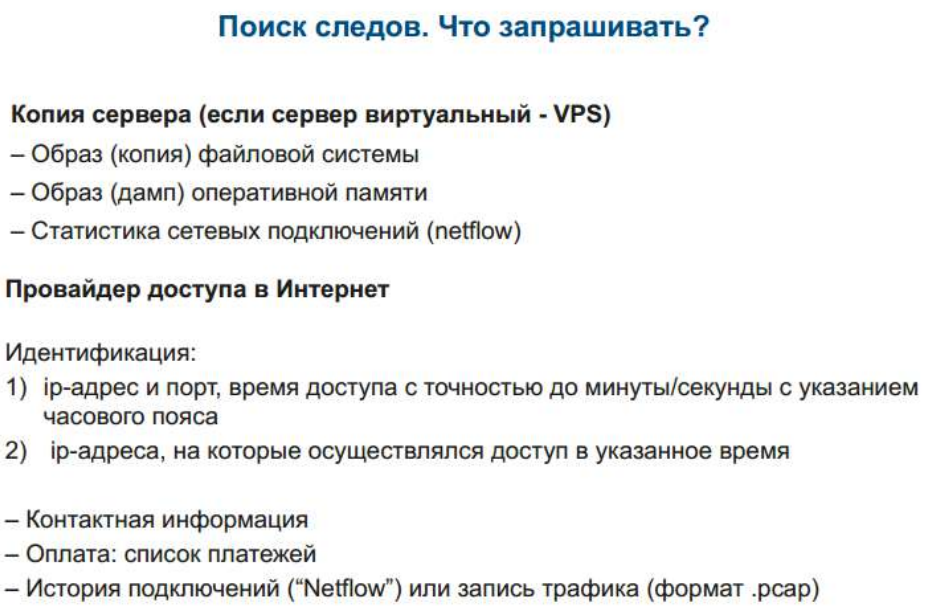


Рис. 5. Поиск следов

Список литературы

1. Официальный сайт Генпрокуратуры Российская Федерация // URL: https://crimestat.ru/offenses_chart (дата обращения: 24.11.2021).

Шишина Е. А.[1]*,*
старший преподаватель кафедры оперативно-розыскной деятельности и специальной техники Крымского филиала Краснодарского университета МВД России

Тарасевич А. В.[2]*,*
слушатель 53 взвода Крымского филиала Краснодарского университета МВД России

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА И НЕКОТОРЫЕ ПУТИ ИХ РЕШЕНИЯ

Сегодня вместе со стихийными бедствиями, войнами, вирусами и эпидемиями, идущими бок о бок с проституцией, наркоманией и голодом, проблема экстремизма и терроризма, обусловленная затяжными кризисом и безработицей в условиях пандемии, набирает все большие масштабы. Активное распространение экстремизма напрямую направлено на подрыв конституционного строя государства, нарушения его целостности и независимости, суверенитета. Зачастую действия экстремистов посягают на дестабилизацию функционирования органов государственной власти и управления, их эффективной деятельности.

В настоящее время проблема экстремизма, подкрепленная нестабильностью в мировом сообществе, вызванной введенными ограничениями в связи с распространением коронавирусной инфекции (COVID-19) [1], набирает все большую актуальность и требует своевременных и эффективных решений. Введение ограничений на передвижение как внутри страны, так и за ее пределами, закрытие или приостановление деятельности большого количества предприятий, закрытие границ и авиасообщения, вынужденная самоизоляция граждан, вызвали экономический кризис и безработицу среди населения, способствуя развитию и распространению экстремизма в Российской Федерации, усилению его взаимодействия с международными террористическими и экстремистскими организациями, международной организованной преступностью, что может привести к расширению и укреплению его инфраструктуры и финансовых возможностей.

Современный экстремизм и терроризм стирает границы отдельных стран и регионов, образуя глобальную проблему. Учитывая нестабильную ситуацию, вызванную пандемией коронавируса, необходимо обратить особое внимание на противодействие экстремизму в сфере информационно-телекоммуникационных систем, в частности сети «Интернет», а также неблагоприятную миграционную ситуацию, которая приводит к дестабилизации рынка труда, социально-экономической обстановки, оказывает негативное влияние на межнациональные (межэтнические) и межконфессиональные отношения [2].

Роль информационно-телекоммуникационных систем в современном обществе с каждым годом все сильнее увеличивается, а введение ограничений и самоизоляция, вызванные пандемией коронавируса, лишь ускорили этот процесс. Ведь мы живем в мире высоких технологий, что в свою очередь порождает новые виды преступлений, уход межличностного общения преступников в информационную среду и выдвигает новые требования к правоохранительным органам в части выявления, пресечения, раскрытия и расследования преступлений.

Сегодня экстремистские организации осуществляют преступную деятельность с помощью закрытых групп в социальных сетях, микроблогах, интернет-форумах, мессенджерах, а также онлайн играх. Для посетителей некоторых страниц и сайтов (закрытые группы и сообщества) доступ может быть ограничен, что в свою очередь усложняет правоохранительный и общественный контроль. Негативно влияют на процесс мониторинга информации экстремистского характера случаи использования искаженного IP-адреса (комбинация цифр, символы которой разделены точками), с помощью промежуточных серверов (прокси-сервер), которые являются звеньями между пользователем и конкретным сервером, причем прокси-серверов может быть несколько [3, с. 35–36].

Однако на существуют и успешно применяются различные методы идентификации пользователя. Например, в научной литературе можно встретить описание таких методов, как воздействие на браузер пользователя, воздействие на сетевое соединение пользователя, анализ активности пользователя в виртуальном пространстве.

Идентификация при помощи воздействия на браузер пользователя возможна вследствие несовершенства программного обеспечения для передачи данных в режиме онлайн. Применение данного метода позволяет установить реальный IP-адрес пользователя, несмотря на попытки его сокрытия.

Воздействие на сетевое соединение, установленное пользователем, основано на изучении записей использования одного из протоколов, работающего на уровне сетевого оборудования. Данный протокол является открытым и создан для мониторинга и анализа сетевого трафика. Создание записи о каждой транзакции является его особенностью. Благодаря этому возможно проведение анализа с целью идентификации пользователя сети.

Анализ активности пользователя в виртуальном пространстве характеризуется рядом особенностей, часть которых связана с его оборудованием. Суть метода заключается в том, что интернет-страницы, просматриваемые пользователем, подстраиваются под его программно-аппаратное обеспечение. Эти сведения позволяют создать цифровой след, который дает возможность в дальнейшем идентифицировать пользователя.

Основной проблемой применения данного класса методов является то, что пользователь может выходить в сеть интернет с разных устройств и мест, а также обновлять программное обеспечение, изменяя, тем самым, его характеристики. В противовес этому наиболее устойчивыми признаками, позволяющими идентифицировать пользователя, выступают его собственные биометрические характеристики. Например, индивидуальным поведенческим биометрическим признаком будет клавиатурный почерк с определенной

скоростью и динамикой ввода символов. В свою очередь, методы идентификации по клавиатурному почерку, также можно разделить на три группы: методы анализа поведения пользователя при авторизации, методы анализа поведения после авторизации, методы постоянного распознавания клавиатурного почерка пользователя. Каждый из них имеет свои положительные качества, но более точная идентификация возможна в ходе непрерывного комплексного мониторинга действий пользователя. Как один из способов реализации такого подхода, можно рассматривать алгоритм, на основе использования наиболее часто встречающихся биграмм (пар букв). Этот способ основан на сборе статистических данных, при котором осуществляется запись временных параметров в момент ввода определенных символов.

Однако, следует учитывать и специфику сетевого пространства, которая характеризуется:

1) Дефицитом времени на принятие решения и осуществление оперативно-розыскного мероприятия, ввиду недолговечности существования информационных объектов и логических каналов, то есть динамичности изменения структуры элементов информационных сетей;

2) Спецификой сформировавшейся социальной среды, которую можно рассматривать как устойчивую совокупность личностей, участвующих в сетевых процессах, связанных между собой общественными отношениями [4, с. 12].

3) Технологической сложностью большинства сетевых процессов и большим объемом данных, которые передаются, хранятся и выявляются в электронном виде;

4) Использованием не стационарных ПЭВМ, а средств мобильной связи, доступ и проведение ряда оперативно-розыскных мероприятий затруднены.

Использование мобильного телефона при осуществлении экстремистской и террористической деятельности может дать и дополнительные оперативные возможности. Так, с целью совершенствования деятельности по противодействию экстремизму, выявления и пресечения деятельности деструктивных сайтов (сообществ) целесообразно применять методы, предложенные А. В. Богдановым:

– использование идентификационного модуля абонента для проверки факта регистрации и последующего получения доступа в личный кабинет абонента оператора беспроводной связи. Указанный метод позволяет получить данные о наличие дополнительных сим-карт, зарегистрированных на интересующее лицо, а также в случаях, не нарушающих законодательство, получить доступ к информации о детализации телефонных соединений абонента. В ряде случаев можно получить доступ к сведениям о движении денежных средств по балансу счета при использовании абонентского номера в качестве электронного средства платежа;

– использование идентификационного модуля абонента для получения информации о регистрации аккаунтов в социальных сетях. Это возможно путем осуществления попыток восстановления пароля или регистрации с указанием абонентского номера сим-карты. В результате осуществления указанного приема возможно получение информации о тайных анонимных страницах и груп-

пах, в которых состоит лицо, представляющее оперативный интерес. Кроме того, в предусмотренных законом случаях возможно оперативное получение информации о полученных и отправленных сообщениях, а также о материалах, размещенных пользователем до совершения преступления;

– использование модуля абонента возможно для получения доступа к аккаунту в программных приложениях – мессенджерах. Это особенно важно, когда абонентское устройство связи не обнаружено или неработоспособно. Доступ к аккаунту позволяет в предусмотренных законом случаях получить информацию о переписке пользователя, а также о дополнительных активных устройствах, на которых может быть сохранена история переписки [5, с. 34].

Таким образом, в условиях затяжного кризиса и безработицы, стихийных бедствий, войн, вирусов и эпидемий, идущими бок о бок с проституцией, наркоманией и воровством, все большие масштабы набирают преступления экстремистской направленности и террористического характера. Однако, в эпоху цифровизации остро встал вопрос информационно-технологических проблем борьбы преступлениям экстремистской направленности и террористического характера. В виду изложенного авторами в статье проанализированы проблемы, возникающие при противодействии указанному виду преступлений, а также систематизированы и охарактеризованы некоторые пути их решения.

Список литературы

1. Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Тульской области // URL: http://71.rospotrebnadzor.ru/content/590/82017/ (дата обращения: 22.10.2021).

2. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // НПП «Гарант-сервис». URL: https://www.garant.ru/products/ipo/prime/doc/74094369/ (дата обращения: 22.10.2021).

3. Предупреждение экстремизма и терроризма в подростковой и молодежной среде: методические рекомендации / [сост. С. А. Буткевич и др.]. Симферополь : Крымский филиал Краснодарского университета МВД России, 2018. С. 35–36.

4. Шишина Е. А. «Хизб ут-Тахрир аль-Ислами», как фактор радикализации населения Республики Крым // Криминалистика: теория и практика : материалы VII Международная научно-практическая конференция, 31 мая 2019 г. Краснодар : Краснодарский университет МВД России, 2019. 12 с.

5. Богданов А. В. Проблемы разграничения оперативной, следственной и криминалистической информаций // Вестник Московского университета МВД России. 2009. № 7. 34 с.

6. Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование// Нижний Новгород, 2015. 501 с.

7. Решение Верховного Суда Российской Федерации от 14 февраля 2003 г. № ГКПИ 03-116 // URL: http://nac.gov.ru/zakonodatelstvo/sudebnye-resheniya/reshenie-verhovnogo-suda-rf-ot-14-fevralya.html (дата обращения: 22.10.2021).

Курина В. Д.[1]***,***
слушатель 972 учебного взвода
факультета подготовки специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Овчинский А. С.[2]***,***
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

ПОЛИТИЧЕСКИЙ ЭКСТРЕМИЗМ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНЫХ СФЕР

На фоне стремительного развития информационных технологий меняются представления об информационной безопасности. На этапе автоматизации, с появлением первых ЭВМ и компьютеров информационная безопасность почти полностью ассоциировалась с обеспечением защищенности собственно информации, автоматизированных систем обработки данных, сетей передачи данных, объектов информатизации.

Развитие цифровых технологий и Интернет-коммуникаций вывело информационную безопасность на орбиту национальной безопасности.

В действующей Доктрине (2016 г.) информационная безопасность – это «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Доктрина, являясь документом стратегического планирования, представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере [1].

Следующий этап развития представлений об информационной безопасности, обусловленный уже цифровой трансформацией, связан с угрозами, которые несут технологии информационных воздействий самым разным сферам общественных отношений. Речь идет о таких сферах как семейные отношения, система образования, организация досуга, сферы культуры, искусства, религии, сферы управления на разных уровнях (государственном, муниципальном, местном), то есть обо всех сферах, построенных на информационных взаимодействиях.

Среди угроз безопасности информационным сферам наибольшую опасность представляет политический экстремизм.

Проблема воздействия политического экстремизма на общество, сферы его жизни и личность в отдельности стоит достаточно остро, учитывая сов-

ременные политические настроения в Российской Федерации и в мире. Это можно заметить по напряженности, сохраняющейся на мировой арене и в пределах нашего государства.

Понятие политического экстремизма в настоящее время не имеет четкой формулировки. Являясь одной из разновидностей экстремизма политический экстремизм в широком смысле – это приверженность в политике к крайним взглядам и действиям. Он выражается в протестах, митингах и массовых беспорядках.

Опираясь на другие исследования можно заключить, что «политический экстремизм – использование радикальных форм и методов борьбы с действующей властью, достижение политических целей крайними методами, вплоть до террористических актов».

Под политическим экстремизмом можно также понимать «незаконную деятельность политических движений и партий, отдельных должностных лиц и граждан, а также государств и их союзов направленную на насильственное изменение существующего государственного строя и на разжигание национальной и социальной розни. Для политического экстремизма в таком понимании характерны три основных момента: нелегитимная политическая деятельность, прежде всего незаконное насилие; крайние формы национализма, расизма или социально-классового антагонизма; простота и общедоступность идеологии» [2].

Одно из наиболее емких определений дано А .С. Зайналабидовым и В. В. Черноусом: «Политический экстремизм – это исторически изменяющееся социально-политическое явление, выражающееся в стремлении определенных политически активных индивидов, общественных групп, властвующих элит и контрэлит воплотить в жизнь свои политические идеалы и реализовать поставленные задачи всеми доступными средствами, включая различные формы насильственного воздействия, направленные на государственную власть, общество в целом или на какие-либо его элементы, международные организации, иные страны и в перспективе на все человечество в целом, а также обосновывающие и оправдывающие это насилие идеологии» [3].

В целом политический экстремизм представляет собой сложный социально-политический феномен, имеющий тенденции к саморазвитию. Появление его обусловлено наличием целого ряда социально-экономических и социокультурных факторов, тесно взаимодействующих между собой.

Важно представлять, что отсутствие одного или нескольких из этих факторов может значительно препятствовать распространению экстремистских настроений и резко понижать воздействие экстремистской идеологии на массовое сознание.

Это можно пояснить на довольно простом примере. Так, если в стране довольно высокий уровень жизни и хорошая социально-экономическая обстановка, то трудно вызвать недовольство граждан и спровоцировать их на протест против политического режима в стране.

Если проанализировать вышеизложенные определения политического экстремизма, то можно сформулировать следующее: политический экстремизм – это исторически изменяющееся негативное явление, выражающееся в деятель-

ности политических движений и партий, отдельных должностных лиц и граждан, а также государств и их союзов, приверженных к крайним политическим взглядам, направленным на распространение своей политической идеологии, а также насильственное изменение существующего государственного строя, сопровождающегося различными формами противоправных действий.

Политический экстремизм как опасное социальное явление находит свое отражение в прошедших событиях отечественной и мировой истории. К ним можно отнести различные протесты, восстания и революции, направленные против существующего государственного строя. Также сюда можно отнести военные акции, направленные на свержение действующих правительств и на нарушение территориальной целостности государств, подкрепленные политической идеологией и иными интересами агрессивной стороны. Не исключено, что и многие террористические акты также имеют отношение к большой игре мировых политических сил.

Политический экстремизм характеризуется:

- противоправностью, выражающейся в массовых беспорядках и протестах;
- воздействием на общество с помощью различных психологических методов;
- пропагандой собственной идеологии, имеющей деструктивный характер.

Таким образом, можно выделить несколько основных признаков деятельности, связанной с политическим экстремизмом: политическая направленность, противозаконность, психологическое воздействие и распространение идеологии.

Если рассматривать опасность, исходящую от политических экстремистов, то их деятельность безусловно представляет угрозу безопасности информационным сферам. Активность политических экстремистов не ограничивается лишь пропагандой своей идеологии. Она связана, например, с искажением и предвзятой интерпретацией исторических фактов.

Главной проблемой современного мира является угрозы, связанные с воздействием на сознание людей, в особенности подростков и молодежи.

Опасность воздействия на них со стороны экстремистов, в том числе политических, что у них нет четко сформированного понимания мира, положения дел и своей роли в системе общественных отношений. Это открывает возможности манипулирования сознанием молодых людей.

Механизмы информационно-психологических воздействий можно рассмотреть, анализируя систему энергоинформационных трансформаций в социальной жизни, представленную на рисунке 1 [4].

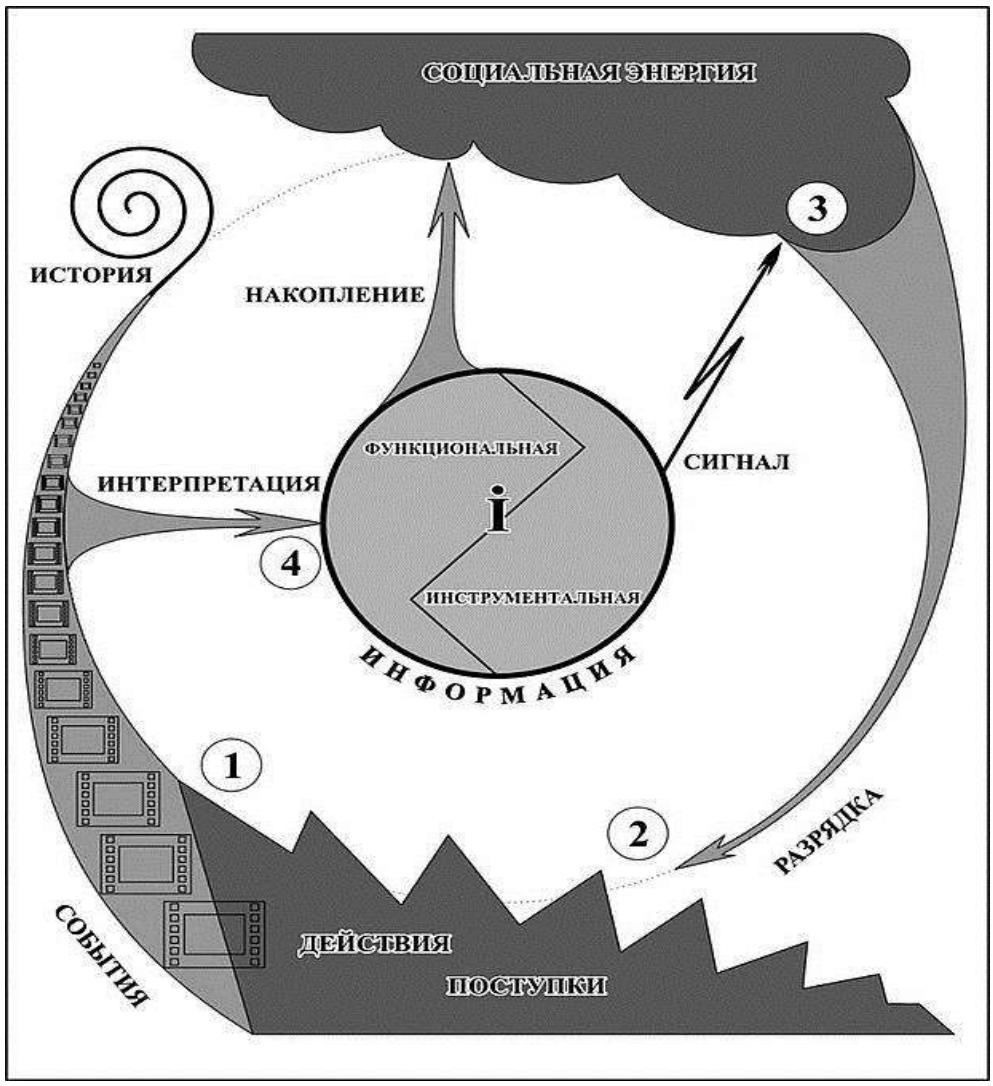


Рис. 1. Система энергоинформационных трансформаций социальной жизни

Опираясь на приведенную на рисунке 1 схему, можно выделить алгоритмы воздействия искаженной информации на сознание человека.

Началом могут стать сообщения, получаемые подростками и молодежью из различных источников, в том числе школьных и вузовских учебников, Интернета, в том числе социальных сетей, СМИ. Полученные сведения обрабатываются сознанием человека. Возникает интерпретация происходящих событий и сообщений о них. При этом ключи интерпретации могут задаваться извне, в частности заказчиками и вдохновителями экстремистских выступлении.

Информация, возникшая в сознании человека переходит в своеобразную энергию действий, энергию общения, когда после интерпретации полученных сообщений и сигналов человек, как социальное существо делится возникшей в его сознании информацией и принимает определенные решения.

На определенном этапе наступает момент разрядки потенциалов накопленной энергии, спровоцированной сигналом извне. Это может произойти в результате определенной провокации. На этом этапе круговорот информации приводит к противоправным действиям, проявлениям политического экстремизма: массовым беспорядкам, несанкционированным митингам, протестам, а в некоторых случаях и к вооруженным конфликтам.

Что касается способов сигнального воздействия, то в современном мире, в отличие от прошлого, распространение политической идеологии кардинально изменилось. Если раньше это осуществлялось с помощью листовок, пропагандистов и приходилось выходить с публичными выступлениями с призывами, то сейчас возможности сигнального воздействия на большие массы людей возросли за счет развития информационно-телекоммуникационных технологий, особенно всемирной сети Интернет.

Современное состояние Интернета способствует более быстрому поиску единомышленников и молниеносному распространению идеологии в социальных сетях.

Деятельность правоохранительных органов в современных условиях в борьбе с политическим экстремизмом должна быть направлена на отслеживание, наблюдение, контроль за циркулируемой в просторах Интернет-пространства информацией, а также на выявление лиц, занимающихся распространением материалов экстремистского характера. Для наиболее успешной борьбы с политическими экстремистами требуются усилия не только правоохранительных органов, но и иных государственных структур.

Список литературы

1. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http:// www.consultant.ru (дата обращения: 22.10.2021).

2. Экстремизм: понятие, виды, ответственность / Управление МВД России по Курганской области // URL: https://45.мвд.рф/document/19145617 (дата обращения 22.10.2021).

3. Сущность политического экстремизма и терроризма / Управа района Бирюлево Восточное города Москвы // URL: http://bv.mos.ru/safety-and-security/antiterroristicheskaia-safety/detail/1686005.html (дата обращения: 22.10.2021).

4. Овчинский А. С. Информационные воздействия и организованная преступность. М. : ИНФРА-М, 2007.

Очилов А. И.[1]*,*
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя

Плотников Г. Г.[2]*,*
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА ЧЕРЕЗ КОМПЬЮТЕРНЫЕ ИГРЫ

XXI в. – век информационных возможностей, охватывающие все сферы жизнедеятельности. Начиная, от обычного общения в социальных сетях и заканчивая покупками различных товаров в интернет магазинах. С появлением таких возможностей, жизнь человека значительно облегчилась, но и появились новые угрозы. И одной из таких угроз является международный терроризм, который является настоящей «раковой опухолью» XXI в. Благодаря, современным возможностям информационных технологий, терроризм расширил свои возможности еще больше. Это способствовало созданию новых методов вербовки через сеть интернет, сохраняя полную анонимность.

Особое внимание нужно обратить на борьбу с финансирования международного терроризма. С каждым днем возникают новые схемы для финансирования терроризма и еще одним новым способом, является финансирование терроризма через компьютерные игры.

Директор Федеральной службы по финансовому мониторингу Юрий Чиханчин на встрече с президентом Российской Федерации Владимиром Путиным рассказал о появлении новой схемы финансирования терроризма — через компьютерные игры в сети интернет.

Как происходит финансирование через компьютерные игры

Существует несколько вариантов возможного финансирования через компьютерные игры:

1. Финансирование происходит путем продажи внутри игрового инвентаря за реальную деньги. На сегодняшний день существуют множество различных онлайн игр, которые популярны среди различных слоев население. Условно, когда вы впервые заходите в игру, ваш игровой персонаж на фоне остальных игроков «ветеранов» очень слаб и уязвим, и играть в таких неравных условиях вам будет очень сложно. И тогда создается взаимовыгодные условия между новичками и ветеранами, где ветераны выставляют в так называемый игровой ры-

нок свой игровой инвентарь в обмен на реальные деньги. А новичок в состоянии азарта совсем не против потратить пару тысяч, а в некоторых случаях даже пару сотен тысяч рублей, лишь бы заполучить свой желанный инвентарь. Именно вырученные деньги за продажу игрового инвентаря и идут на финансирование террористов.

2. Вторым способом, является, взлом игровых аккаунтов. Данный способ более сложный в исполнении, так как чтобы провернуть данную махинацию требуются немало усилий. Достаточно большое количество игроков при регистрации не уделяют должного внимания сложности пароля в отличие от регистрации в социальных сетях или в других приложений. И именно, такие пароли легко взломать путем обычного подбора пароля. Так же существуют множество фишинговых сайтов, где наивных игроков привлекают на приобретение «премиальных» игрового инвентаря по более низким ценам.

3. Третьим способом является использование игровой валюты для совершения транзакции с дальнейшей монетизацией.

4. Создание игровых серверов самими террористами. Помимо официальных игровых серверов в сети интернет существуют множество пиратских серверов, администраторами которых могут является сами террористы.

5. Еще одной большой проблемой является использование для покупок криптовалюты. Данный способ относится не только для совершения транзакции через игры в интернете. Например, террорист принимает оплату в биткоинах в свой криптовалютный кошелек, затем совершает ввод в любой интернет сервис, который поддерживает оплату по криптовалюте и сразу же выводит их, но теперь уже в обычной валюте.

К сожалению, на сегодняшний день не существует каких-либо конкретных мер пресечения данной схемы. Еще одной глобальной проблемой, является то, что онлайн игры с каждым годом набирают еще большую популярность. CEO агентства Insight ONE в 2014 г. привели статистику об игровой индустрии в России. По статистическим данным 58 % Россиян играют в онлайн игры, где средний возраст составляет 30 лет. Сейчас процентное соотношение выросло еще больше. С увеличением популярности увеличивается и финансовый оборот в игровом пространстве. Так как для разработки технической системы защиты от данной схемы махинации требуется время, оперативным решением для воздействия на данную схему будет разработка конкретной правовой защиты. Еще одним значимым методом может послужить профилактические лекции в местах учебы. А что касается технической защиты, то можно создать антипиратскую систему, которая будет блокировать нелицензированные игровые серверы, а на лицензированных серверах создать единую игровую валюту, транзакции которых можно отследить. Еще одним эффективным способом будет являться отказ от использования криптовалюты. Но данные методы могут лишь только ча-

стично ослабить данную схему, так как для полного пресечения финансирования терроризма в сети интернет нужно будет поступать более радикально.

Список литературы

1. Терроризм как объект противодействия в системе обеспечения информационной безопасности: международные и организационно-правовые аспекты» // Вестник академии экономической безопасности МВД России, 2011.

2. Исследование Insight ONE». Игровая индустрия в России // Статистика CEO агентства Insight ONE. URL: https://vc.ru/flood/4236-game (дата обращения: 26.06.2014).

Бекмурадов Х. Г.[1]**,**
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя

Зарипова Э. Р.[2]**,**
доцент кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИСТСКОМУ КОНТЕНТУ В СОЦИАЛЬНЫХ СЕТЯХ

Интернет сегодня является наиболее доступным способом получить информацию. Можно узнать, как проехать из точки А в точку Б, можно оставить объявления о пропаже собаки в социальных сетях, узнать о своих конституционных правах. Многие ресурсы в Интернете не требуют обязательной идентификации личности и разрешают оставлять отзывы или объявления, и даже создавать паблики без проверки личности и местонахождения человека. Любое информационное пространство собирает вокруг себя подписчиков, поклонников и просто интересующихся.

Крайне незащищенными являются подростки и молодые люди с малым жизненным опытом, не вполне осознающие последствия своих действий. Молодые люди в рамках семьи, возможно, имеют малую свободу, и хотят стать более самостоятельными, ищут способы жить отдельно, поехать в другую страну, ищут новых кумиров, которые помогут осуществить им мечту быть более самостоятельными.

Информация сегодня подается разносторонне и под разными углами, и в конце концов достигает своего читателя и слушателя. Большая часть информации сегодня воспринимается глазами, меньшая часть – ушами. В информационном пространстве мало регулирования, есть возможность загружать видео и текстовую информацию, например, в YouTube или в социальные сети без какой-либо ответственности.

На территории Российской Федерации за период январь-сентябрь 2021 года зарегистрировано 854 преступления экстремистской направленности [1], в тройку антилидеров входят республика Дагестан – 47 преступлений, Кемеровская область и г. Москва – по 42 преступления. За весь 2020 год в Российской Федерации было зарегистрировано 833 преступления, т.е. за первые 9 месяцев 2021 года по количеству преступлений экстремисткой направленности зарегистрировано больше преступлений, чем за 12 месяцев прошлого года. Необходимо упомянуть, что за первые 9 месяцев 2021 выявлено 694 лица, совершивших преступления экстремистского характера, хотя за 12 месяцев 2020 года выявлено только 664 человека [1].

В качестве примера на 2021 год авторы выделяют ярко выраженную ситуацию в Афганистане. Захват Афганистана талибами произошел после ухода американский войск, в настоящее время талибы полностью контролируют эту страну. Через средства массовой информации талибы пополняют свои ряды, им нужны люди, выполняющие указания в разных точках мира. Такие последователи делают экстремистов непредсказуемыми и вездесущими. Подростки и молодые люди могут быть завербованы разными способами: через своих знакомых, родственников или на финансируемых вербовщиками мероприятиях, иногда через давление и угрозы жизни и здоровью близких. Одним молодым людям могут предложить финансовую или другую помощь, другим пригрозить обнародованием компромата, третьи готовы сотрудничать с экстремистами по идейным соображениям, разочаровавшись в своих собственных убеждениях.

Информация от самих экстремистских группировок подается вовне как положительная для привлечения новых людей, в том числе и подростков. В широко распространенных социальных сетях у уже упомянутых талибов есть свои аккаунты, где они публикуют свои новости. У этих аккаунтов образуются подписчики, с которыми под разными видами могут переписываться специально обученные вербовке люди. Вступить в подобную «секту» легко, произнеся определенную клятву верности. В этот момент наемнику говорят то, что он хочет услышать, о его принадлежности к сильному сообществу. Если реальное окружение молодого вербуемого не устраивает его по каким-то причинам, то ему действительно хочется коротким путем быть причастным к глобальным действиям.

Авторы противостоят идее терроризма и экстремизма в информационном пространстве и, в частности, любому экстремистскому контенту. Большую роль играют государство и силовые структуры, запрещающие распространение экстремистского контента в социальных сетях, поскольку от действий экстремистов и их последователей могут пострадать и мирные жители.

Авторы считают наиболее уязвленным молодое поколение в возрасте 14–22 лет и предлагают со школьного возраста проводить беседы со школьными и приглашенными психологами, которые могут в доверительной беседе или при работе с классом обсудить реальные ситуации вербования, алгоритм обращения в правоохранительные органы при случаях вербовки, дать телефоны горячей линии для обращения.

Необходимо демонстрировать все этапы вербовки молодых людей, как могут развиваться события, и чем они по статистике заканчиваются, обязательно озвучивать наказание за финансирование террористических группировок и участие в экстремистской деятельности, нарушение Федерального закона Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» [2]. Реальная ситуация с терроризмом меняется каждый день, как мы видим это на примере Афганистана в 2021 г., страдают все жители, особенно женщины и несогласные с талибами. Психологи, работающие с молодым поколением, а также все приближенные к данному вопросу должны иметь актуальные методики работы с населением, проходить профессиональную переподготовку.

С другой стороны, необходимо заполнять досуг молодых людей спортивными кружками, увлекательной научной деятельностью, работать с молодежью, вовлекать их в трудовую деятельность.

Немаловажным является и фильтрация допустимого контента в социальных сетях, блокировка отдельных аккаунтов и пабликов, призывающих к террористической и экстремистской деятельности. Кроме того, мир начинается с нас самих, будем внимательны к своей семье, к своим близким и знакомым.

Список литературы

1. Портал правовой статистики // URL: http://crimestat.ru/offenses_chart (дата обращения: 13.11.2021).

2. Федеральный закон Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102105192 (дата обращения: 13.11.2021).

Гриднева И. П.[1]*,*
курсант 281 взвода факультета сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В. Я. Кикотя

Тутынин И. Б.[2]*,*
доцент кафедры уголовного процесса
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ СЛЕДОВАТЕЛЯМИ НОРМ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ПРАВА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Российское общество XXI века столкнулось с мировой проблемой, связанной с резким технологическим развитием. Сейчас происходит активная цифровизация общества, развитие виртуальных экономических отношений и появление новых финансовых рынков и сфер интересов.

Перед современными правоохранительными органами всех стран мира возникла необходимость адекватного и эффективного реагирования на новые угрозы государства, общества и отдельно взятого человека, исходящие от преступлений, совершаемых посредством транзакций криптовалют. Поэтому многие государственные правоохранительные системы разрабатывают новое законодательство, новые схемы и методики для того, чтобы эффективно раскрывать и бороться с такими новыми типами преступлений.

Современная правоохранительная деятельность справляется с “типичными” нарушениями уголовного законодательства: преступления против личности, кражи, разбойные нападения и другие преступные посягательства, в которых наработан практический опыт и имеется достаточно регулируемая законодательная база.

Наиболее частыми преступлениями, совершаемыми дистанционно, выделяют такие как мошенничество, финансирование терроризма, незаконный оборот наркотических средств, огнестрельного оружия, торговля людьми и человеческими органами, а также легализация (отмывание) доходов, добытых преступным путем [9].

В отчетном периоде за 2020 г/ число преступлений, совершенных с использованием информационно – телекоммуникационных технологий, возросло на 73,4 %, в том числе с использованием сети Интернет – на 91,3 %, при помощи средств мобильной связи – на 88,3 % [2].

С появлением вышеперечисленных цифровых технологий, возникают некоторые проблемы правоприменения уголовно – процессуального законодательства о возможности применения меры процессуального принуждения в виде наложения ареста на имущества в отношении криптовалют, а также следствен-

ных действий, в ходе которых приходится обращаться с цифровыми финансовыми активами.

Следователи сталкиваются в своей практической деятельности с недостатком юридической практики и несовершенством уголовно-процессуального законодательства. Нерешенность статуса виртуального имущества и существующие пробелы в Уголовно-процессуальном кодексе Российской Федерации (далее – УПК РФ) затрудняют производство следственных действий, возникают отдельные проблемы применения мер процессуального принуждения.

Одним из ярких примеров, вызывающим сложность для российских следователей, являются ст.ст. 174 и 174.1 Уголовного кодекса Российской Федерации (далее – УК РФ), то есть легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления. Современные преступники легализуют свой доход, добытый преступным путем, используя криптовалюту.

Также совершаются преступления, связанные только с криптовалютой или же ее оборотом: например, кражи и мошенничества.

На данном этапе в российском законодательстве отсутствует четкое определение такого понятия как криптовалюта, что мешает не только квалифицировать преступления, но и при производстве следственных действий.

Сейчас многие ученые и юристы – практики трактуют определение криптовалюты как цифровой валюты, которая закреплена в ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». В п. 13.1 ст. 5 УПК РФ криптовалюта не указана, но в соответствии с данной нормой ее можно понимать как имущество. В статье 141.1 Гражданского кодекса Российской Федерации (далее – ГК РФ) криптовалюта может пониматься как цифровые права. Непосредственное упоминание криптовалюты есть в Постановлении Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» как денежные средства, приобретенных в результате совершения преступления [10].

Присоединяюсь к мнению ученых и юристов – практиков, считаем, в национальной системе права понятие криптовалюта не конкретизирована и четких регламентируемого правового статуса не имеет.

Исходя из анализа вышеперечисленных нормативно правовых актов, можно прийти к выводу, что на данный момент в российском праве криптовалюта находится в «серой» зоне, то есть отсутствует возможность государственного контроля регулирования обращения данного явления, при этом ярко выражена анонимность как пользователей, так и анонимная возможность совершения любых сделок. Не урегулированная правовая природа криптовалют – как цифровая валюта, средство платежа, имущество или еще что-либо. Но полностью запретить обращение криптовалюты не представляется возможным из-за технических, правовых и экономических причин. Криптовалюта, хотя и появилась

совсем недавно, но уже полностью интегрировалась в жизнь потребителей, затрагивая многие экономические процессы.

У нас вызывает озабоченность исчерпанность правового регулирования Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», УПК РФ и ГК РФ. Законодательство не позволяет совершить законные и обоснованные процессуальные действия (следственные действия и меры процессуального принуждения).

Следовательно, необходимо определить правовую природу криптовалюты. Представляется, таковой является – средство платежа. Для потребностей применения УПК РФ это обяжет законодателя разработать соответствующий уголовно-процессуальный инструментарий.

Таким образом, для эффективного противодействия преступлениям, связанным с использованием криптовалюты, необходимо образовать симбиоз трех элементов (технологический, правовой, экономический) и наладить этот механизм среди практических органов. В первую очередь урегулировать правовую и процессуальную базу, а затем обеспечить организационно-техническое исполнение законов.

Список литературы

1. Brenig C., Accorsi R., Müller G. Economic analysis of cryptocurrency backed money laundering // URL: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1019&context =ecis2015_cr (date of access: 29.10.2021).

2. Статистика и аналитика. Раздел «Краткая характеристика состояния преступности в Российской Федерации за 2020 год» // URL: мвд.рф/reports/item/.

3. Рекомендации ФАФТ по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения // URL: http://www.fatf-gaii.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Russian.pdf.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 22.08.2021) г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_law_10699/ (дата обращения: 25.10.2021).

5. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.07.2021, с изм. от 23.09.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 25.10.2021).

6. Федеральный закон от 10 декабря 2003 г. № 173-ФЗ (ред. от 02.07.2021) «О валютном регулировании и валютном контроле» (с изм. и доп., вступ. в силу с 22.08.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_45458/.

7. Постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 “О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имуще-

ства, заведомо добытого преступным путем”» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_319191/ (дата обращения: 25.10.2021).

8. Федеральный закон Российской Федерации от 7 августа 2001 г. № 115-ФЗ (ред. от 02.07.2021) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изм. и доп., вступ. в силу с 28.10.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 25.10.2021).

9. Земцова С. И. Криптовалюта в незаконном обороте наркотических средств: вопросы деанонимизации и ответственности // Криминалистика : вчера, сегодня, завтра. 2020. № 1. С. 54–62.

10. Перов В. А. Проблемные вопросы, возникающие при расследовании уголовных дел о преступлениях с использованием криптовалюты // Российский следователь. 2020. № 7. С. 17–21.

11. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Абрамов А. С.[1]*,*
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Дворянкин О. А.[2]*,*
старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ВЛИЯНИЕ РАДИКАЛЬНЫХ МУЗЫКАЛЬНЫХ ГРУПП НА ПОЯВЛЕНИЕ ЭКСТРЕМИСТСКИХ ОРГАНИЗАЦИЙ В ИНТЕРНЕТЕ

В последние годы отмечается активизация ряда экстремистских движений, которые вовлекают в свою деятельность молодых людей, посредством репертуара различных музыкальных групп и артистов.

По данным экспертов, за последние пять лет, в результате пресечения экстремистских групп, установлено, что членами неформальных организаций (группировок) экстремистско-националистической направленности являются молодые люди от 14 до 18 лет, но есть люди в возрасте до 30 лет.

Субъектами преступлений выступают в основном юноши, но в последнее время и очень часто являются девушки. Они в силу ряда социально-психологических, физиологических и демографических особенностей наиболее восприимчивы к идеологическому воздействию, подвержены максимализму и радикальным настроениям.

В этой связи одним из «активных» воздействий являются музыкальные произведения, авторы, которых завуалированно или открыто призывают слушателя к экстремистским действиям, а также распространяют свою идеологию, например, Моргенштерн (Morgenshtern) российский рэп- и поп-исполнитель, музыкант, шоумен.

Главной проблемой такого воздействия является его массовость и доступность, так как опубликовав аудиозапись в сети Интернет, остановить ее распространение почти невозможно из-за неограниченного копирования в различных интернет-ресурсах.

Таким образом, пользуясь «определенной безнаказанностью» радикальные музыкальные группы и отдельные исполнители провоцируют появление экстремистских организаций в интернете с привлечением в их ряды молодых людей.

В результате борьба с творчеством радикальных музыкальных групп в нынешних условиях возможна, и, очень часто, только на лицензионных платформах, которые соблюдают требования международного и российского законодательства.

Данные платформы удаляют из своих ресурсов данные аудиозаписи после признания их экстремистскими, а также их измененные версии или исполненные другими музыкантами.

Однако полностью блокировать доступ к аудиозаписям пока не представляется возможным, так как существует громадное количество интернет-ресурсов, которые по тем или иным причинам не подчиняются требованиям российского законодательства. Значительная их доля находится в даркнете, но помимо этого есть большое количество торрент-сайтов, на которых запрещенные произведения размещены в свободном доступе.

Примерами недавно запрещенных аудиозаписей могут стать:

1. Аудиозапись «Крада – Белый Штурм» длительностью 2 мин 47 с, начинающаяся со слов: «Четче шаг! Врата небес открыты…», размещенная в сети Интернет. Признана экстремистской Центральным районным судом г. Тулы 31.08.2021.

2. Аудиозапись «Гимн негров» (исполнитель «Дай дорогу»), продолжительностью 2 мин 39 с и начинающаяся словами «Эта мелодия станет гимном для всех…» и заканчивающаяся словами «… Выгонять из России…». Признана экстремистской Октябрьским районным судом г. Белгорода 09.07.2021.

3. Аудиозапись и текст песни под названием: «А.У.Е. Жизнь ворам (За людское) (исполнитель: Вася «Шмель», Лицо Под-Капюшоном, Руслан Черный), длительностью 4 минуты 39 секунд, начинающиеся со слов «Хулиганский двор…» и заканчивающиеся словом «Вечно», размещенные в информационно-телекоммуникационной сети «Интернет». Признана экстремистской Ленинским районным судом г. Владикавказа РСО-Алания 24.05.2021.

При этом необходимо отметить, что представляемый музыкальный репертуар и навязываемая через него экстремистами система взглядов является привлекательной для определенного населения нашей страны (люди проживают в дотационных и депрессионных регионах, некачественный уровень образования, «отсутствие» культуры, низкие заплаты, отсутствие перспектив социального роста и т.д.), в силу простоты и однозначности своих постулатов, обещаний возможности незамедлительно, сей же час, увидеть результат своих пусть и агрессивных действий. Кроме этого они отмечают, что нет необходимости в личном участии в сложных и кропотливых процессах (экономическом, политическом и социальном развитии), и при этом все вышеотмеченное подменяют примитивными призывами к полному разрушению существующих устоев и замены их утопическими проектами.

Таким образом можно отметить, что большое количество музыки разных жанров и Интернет сейчас являются общедоступными инструментами и технологиями в настоящей стране, и молодые люди не всегда могут сразу правильно и верно оценить, что они слушают и понять идеологию авторов, представляющих различный репертуар.

В результате, «авторские» произведения приводят к тому, что в последнее время значительное количество молодых людей и несовершеннолетних, не осознают, что они могут совершить и совершают преступления экстремистского характера.

Поэтому в целях пресечения экстремистской преступности и обуздания криминальной ситуации в данной сфере представляется целесообразным усилить профилактическую работу среди молодежи, в том числе несовершеннолетних путем проведения мер воспитательно-профилактического характера. Подросткам следует рассказывать об формах и особенностях экстремизма, путем проведения просветительских мероприятий (занятий, просветительских программ и семинаров) с представителями органов внутренних дел организации.

В заключение считаем необходимым отметить, что необходимо активизировать предупредительно-профилактическую работу по отслеживанию и принятию мер к ликвидации экстремистско-националистических и экстремистско-террористических сайтов, аккаунтов в социальных сетях, мессенджерах, видеохостингах в интернете, выявлению артистов и музыкальных групп, активно пропагандирующих идеологию экстремизма, а так же публикующих экстремистские материалы, содержащих призывы к совершению преступлений экстремистской и террористической направленности против людей другой национальности или вероисповедания, иностранных граждан, а также подробные инструкции по изготовлению взрывных устройств, совершению террористических актов, «националистических» убийств и т.п.

Список литературы:

1. Особенности профилактики и борьбы с проявлениями экстремизма в молодежной среде // URL:https://cao.mos.ru/countering-extremism/features-for-the-prevention-and-suppression-of-manifestations-of-extremism-and-terrorism-in-the-yout/ (дата обращения: 05.12.2021).

2. Федеральный список экстремистских материалов // URL:http://pravo-minjust.ru/extremist-materials (дата обращения: 05.12.2021).

3. Деструктивные музыкальные группы и их влияние на подростков // URL:http://oroik.by/destruktivnye-muzykalnye-gruppy-i-ix-vliyanie-na-podrostkov/ (дата просмотра 5.12.2021).

Баринова А. К.[1]*,*
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Думачев В. Н.[2]*,*
доцент кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук, доцент

КВАНТОВЫЕ КАНАЛЫ СВЯЗИ, КАК СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ

На сегодняшний день с получением и передачей информации связана вся жизнедеятельность современных людей. На данный момент она является тактическим ресурсом государств и общества в целом, который нуждается в сохранении и защищенности от неправомерных действий, приводящих к ущербу. Если говорить о методах обеспечения защиты информации, то их существует немалое количество, но при всем этом возникают новые угрозы для информационной безопасности. Одной из таких является получение информации пут ем перехвата ее по каналам связи. Решение таких задач требует качественных изменений и перехода научной криптографии на новый уровень информационной безопасности. Ввиду этих проблем и было порождено новое направление в сфере защиты информации – квантовая криптография.

Квантовая криптография – технология, использующая квантовую физику для обеспечения надежной защиты информации. В отличии от классической криптографии, которая пользуется математическими методами защиты информации, квантовая криптография сосредоточена на физике и рассматривает случаи, когда информация переносится с помощью объектов квантовой механики.

Принципы работы квантовой криптографии можно объяснить, рассматривая передачу информации с помощью одиночных фотонов, которые являются квантовыми частицами света, передаваемыми по оптическому каналу, так называемыми кубитами. Особенность кубита заключается в том, что он представляет собой линейную комбинацию состояний квантового бита. При выполнении унитарных операций над кубитовой квантовой системой, которая находится в состоянии суперпозиции, происходит одновременная обработка всех возможных событий. Такой эффект позволяет хранить большое количество информации и дает значительное ускорение вычислительных процессов. Квантовое распределение ключей, которое очень тесно связано с квантовой криптографией, является методом безопасной связи, реализующим криптографический протокол, включающий компоненты квантовой механики. Квантовое распределение ключей и другие протоколы квантовой криптографии используют принципы квантовой механики для обеспечения защищенной криптосистемы с открытым

ключом. При этом, если в канале связи будет подслушивающее устройство, которое пытается узнать секретный ключ, то эти протоколы смогут обнаружить его присутствие.

На сегодняшний день большое количество информации, которая переда ется по каналам связи, шифруется с использованием криптографических систем с открытым ключом. В таких системах ключ состоит из двух частей: открытой и секретной (закрытой). Данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с помощью закрытого ключа, а данные, зашифрованные с помощью закрытого ключа, могут быть расшифрованы только с помощью открытого ключа. Безопасность криптографии с открытым ключом основана на предположении о сложности некоторых задач, таких как целочисленная факторизация и дискретная логарифмическая задача. Это делает систему потенциально уязвимой для повышения вычислительной мощности или обнаружения эффективных алгоритмов. Чтобы этого избежать, Чарльзом Беннетом и Жилем Брассаром в 1984 году был разработан алгоритм кодирования и передачи сообщений, который впоследствии был назван протоколом квантовой криптографии – BB84.

Кратко рассмотрим принцип работы данного алгоритма, который позволяет двум пользователям создать общий криптографический ключ. Он основан на идеях поляризации фотонов. Ключ состоит из битов, которые передаются как фотоны. Базовая модель квантового распределения ключей состоит из двух сторон, называемых Алисой (отправителем) и Бобом (получателем), имеющих доступ как к квантовому каналу связи, который является частным и предполагает совместное использование секретного ключа путем обмена квантовыми частицами, так и к классическому каналу связи, который является открытым и включает в себя базовое согласование, исправление ошибок и протоколы усиления конфиденциальности.

Предполагается, что подслушивающий, называемый Евой, может получить доступ к обоим каналам.

Рис. 1. Базовая модель квантового распределения ключей

В первой части протокола Алиса берет единичный фотон и поляризует под одним из четырех углов: 0°, 45°, 90° или 135°. Полагается, что Алиса сначала

выбирает базис поляризации («+» или «×»), а затем выбирает в этом базисе одно из двух направлений поляризации:

- 0° («↑») или 90° («→») в первом базисе-ортогональном;
- 45° (« ↗ ») или 135° (« ↙ ») во втором базисе-диагональном.

При этом при битовом вычислении при 0° и 45° будет 1, а при 90° и 135° – 0

Алиса может закодировать бит распределяемого ключа в состоянии квантовой частицы и отправить Бобу. Перехватчик (Ева) не сможет достоверно узнать, какое состояние было отправлено, а ее попытки произвести измерения и определить какие биты были отправлены, неизбежно приведут к изменениям в состояниях пересылаемых квантовых битов. В результате отправленная Алисой и измеренная Бобом строки бит будут отличаться. Если после сеанса передачи Алиса с Бобом выделят в битовой строке статистически значимое множество и публично произведут сверку бит, они смогут определить долю ошибок и, руководствуясь моделью, ограничить сверху возможное вмешательство Евы.

В случае, если полученный уровень ошибок не позволяет гарантировать секретность передаваемого ключа, такая строка бит не используется для шифрования. В результате, на руках у перехватчика остается только случайный набор чисел, не имеющий никакого применения.

Битовая строка Алисы	1	0	0	1	1	0	1	0	0	1
Поляризация Алисы	↗	↖	→	↗	↑	→	↑	↖	→	↗
Базис Боба	+	+	x	+	+	x	+	+	+	x
Расшифрованный ключ	0	1	1	0	1	0	0	0	1	0

Рис. 2. Протокол BB84

Квантовая криптография безоговорочно защищена в том смысле, что не делается никаких предположений о неспособности Евы решать сложные математические задачи, а скорее о ее неспособности нарушать принципы квантовой механики. Однако эти протоколы уязвимы для атаки "человек посередине", когда Ева притворяется Бобом или Алисой. Такие атаки невозможно предотвратить без того, чтобы Алиса и Боб сначала не аутентифицировали друг друга. Кроме того, квантовая криптография не является полностью защищенной при использовании с неисправным оборудованием и в шумной среде. В квантовом канале, подверженном ошибкам, для разработки защищенного ключа можно использовать согласование информации и усиление конфиденциальности. Таким образом, нельзя безоговорочно говорить об идеальности криптографического протокола BB84.

Квантовые каналы связи являются базисом для реализации алгоритмов квантового распределения ключей. Преимущество таких каналов – распределение ключей на большие расстояния между пользователями по открытым каналам связи, при этом у посторонних людей, которые не участвуют в передачи,

нет возможности скопировать неизвестное квантовое состояние, прослушать сигнал и различить два не ортогональных квантовых состояния.

Квантовая криптография – метод защиты информации будущего. В настоящее время ни квантовые вычисления, ни квантовая криптография не находятся на той стадии, когда они могут быть практически применены. До сих пор мощное использование квантового компьютера для расшифровки и шифрования информации работает только в теории, поскольку такие компьютеры очень большие по размеру и могут быть изготовлены только на заказ. Так же стоит сказать, что данные алгоритмы работают на ограниченных расстояниях, при превышении 50 км между ними, шум становится настолько великим, что частота ошибок стремительно растет. Сейчас многие государства, в том числе и Россия, вкладывают большие средства в развитие этого направления и решения технических задач, поскольку все понимают, что после создания квантового компьютера классическая криптография станет неэффективным способом защиты информации. Когда же квантовые компьютеры введут в оборот, вычислительные скорости резко возрастут, и математическая сложность алгоритмов классической криптографии станет менее сложной задачей. По всему вышесказанному можно сделать вывод о том, что квантовая криптография – очень перспективное направление, являющееся настоящим прорывом в области информационной безопасности, которое не стоит на месте, развивается и является одним из самых действенных способов защиты информации.

Список литературы

1. Леденев А. Н. Физика. В 5 книгах. Книга 1. Механика. М. : ФИЗМАТЛИТ, 2005. 240 с.

2. Нильсен М., Чанг И.. Квантовые вычисления и квантовая связь. М. : Мир, 2006.

3. Дуплинский А. В. Квантовое распределение ключа с высокочастотным поляризационным кодированием : дис. … канд. физ-мат. наук : 01.04.21. М., 2019. 102 с.

4. Квантовая криптография // URL: https://se7en.ws/kvantovaya-kriptografiya-prosteyshie-protokoly-i-chut-chut-kriptoanaliza/ (дата обращения: 18.11.2021).

Хорзова И. С.[1]**,**
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя,

Пакляченко М. Ю.[2]**,**
старший преподаватель кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,

ПРИМЕНЕНИЕ КИБЕРПОЛИГОНА ДЛЯ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ

Одной из значимых угроз современности ввиду цифровизации общества является кибертерроризм, который среди прочего проявляется и в кибератаках на значимые для государства информационные ресурсы и инфраструктуры. К способам борьбы с ними относят многоэлементный арсенал тактик, техник и средств, а также отдельным направлением выделяют обучение и подготовку квалифицированных кадров.

Приходится признать, что в сфере обеспечения защиты данных, в том числе в части противостояния преступлениям, совершаемым в глобальном сетевом пространстве, наблюдается нехватка квалифицированных специалистов не только с теоретическими знаниями, но и с практическим опытом работы по защите от кибератак, а также прикладных средств противостояния киберугрозам [1]. Для этого необходима определенная инфраструктура, позволяющая эмулировать атаки (которые могут отождествляться с активными действиями кибертеррористов) и дающая возможность воспроизводить офицерам безопасности оперативное реагирование на них.

Для реализации отмеченной цели востребовано применение киберполигона, который представляется как технологическая база для моделирования реальных участков информационной инфраструктуры, позволяющая проводить учения по вопросам обеспечения информационной безопасности.

Стоит отметить отсутствие устоявшегося определения для термина «киберучение». Как правило, в российском сообществе в сфере кибербезопасности под данной дефиницией понимают некое практическое мероприятие для отработки командных действий по реагированию на инциденты. Иногда указанные мероприятия именуют «киберполигон». В рамках указанных действий проводится симуляция различных типов атак на некую виртуальную инфраструктуру, где специалисты кибербезопасности оттачивают свои навыки противодействия угрозам и получают новые знания, а также выявляют слабые стороны. Форматы проведения киберучений могут быть разными, например, штабными, функциональными, полномасштабными учениями.

Согласно Постановлению Правительства Российской Федерации [2] под киберполигоном понимают инфраструктуру для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них.

Иными словами, киберполигон – это «виртуальное пространство», агрегирующее в себе теорию и практику в направлении информационной безопасности, используемое для подготовки специалистов в части противостояния актуальным угрозам информационной защищенности, характерной для определенной цифровой среды.

С практической стороны своей реализации киберполигон одновременно может поддерживать работу более сотни виртуальных машин, а также осуществление хранения данных большого объема. Сам проект киберполигона основан на накопленном мировом опыте, так называемых, лучших практиках, интегрирует в себе достигнутые результаты научно-исследовательских лабораторий мирового уровня в сфере защиты информации.

Отличие киберполигона от стандартной виртуальной лаборатории состоит в процессорной сущности: он допускает эмуляцию процессов и инфраструктуры данных стандартных учреждений разнообразных сфер и отраслей деятельности общества и государства (финансовый сектор, коммуникация, производство, энергетика, транспорт, и др.), которые могут быть привлекательными для кибертеррористов. Участникам киберучений предоставляются разнообразные технологии и широкий инструментарий для приобретения и оттачивания прикладных компетенций по защите от кибератак, расследованию инцидентов, ведению реактивной работы в режиме реального времени.

Основной целью функционирования киберполигона выступает стремление к созданию строгого понимания приоритетного значения обеспечения информационной безопасности, которое будет определять степень зрелости любой организации. При проектировании киберполигона преследуются задачи, которые ориентированы на подготовку специалистов в области информационной безопасности, а также обучающихся по данному направлению, а также на проведение контроля и оценку эффективности средств защиты, программного обеспечения, иных элементов информационных систем, подверженных угрозам, среди которых могут быть и террористические атаки.

Таким образом, создание и применение кибеполигонов является одним из оптимальных решений в части подготовки специалистов соответствующего профиля и повышения их знаний, умений и навыков. В процессе эксплуатации киберполигона офицеры информационной безопасности лучше понимают методы, которые используют хакерские и террористические группы, а также получают возможность противостоять им на практике. Выполняется эмуляция атак, вместе с которой происходит отработка компетентностных навыков по их отражению. Причем алгоритмически все выполняется в реальной хронологии: вторжение извне в периметр защищаемой инфраструктуры, передвижение по сетевому периметру и повышение привилегий, приобретение атрибутов сетевого кон-

троля с возможностью администрирования, воздействие на защищаемую информацию, иные варианты сценариев инцидентов информационной безопасности.

Подобная работа в гиперреалистичной среде, включающей в себя настраиваемую сеть защищаемой информационной инфраструктуры, корпоративный инструментарий безопасности, эмулированный информационный поток и симулированные атаки разнообразных сценариев и сложности. Имеющиеся стратегии имитируют наиболее известные и частые в своей реализации киберугрозы. Различные топологии сети могут быть развернуты согласно необходимости действительного положения дел с целью доскональной и максимально реалистично воспроизвести инфраструктуры, которые могут находиться, например, в бюджетных учреждениях, комплексах промышленного сектора и других чувствительных предприятиях, которые требуют обеспечения своей защиты от различного рода угроз, в том числе кибертеррористической природы.

Список литературы

1. Белоус А. И., Солодуха В. А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М. : Техносфера, 2021. 482 с.

2. Постановление Правительства Российской Федерации от 12 ноября 2019 г. № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки, специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения информации» // URL: https://base.garant.ru/72861698/ (дата обращения: 20.10.2021).

Дворянчук Е. А.[1]***,***
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Е. Н.[2]***,***
доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,

СОЦИАЛЬНЫЕ СЕТИ КАК ИНФОРМАЦИОННЫЙ РЕСУРС ДЛЯ ПРОПАГАНДЫ ЭКСТРЕМИСТСКОЙ ИДЕОЛОГИИ И ВЕРБОВКИ НАСЕЛЕНИЯ

Распад Советского Союза привел к тому, что вместо одного сильного, могущественного государства, образовалось пятнадцать независимых. Одним из таких государств и стала Российская Федерация, т.е. мы можем говорить о том, что с конца прошлого века началось новое развитие нашей страны. Переход от одной страны к другой сопровождался разрушением устоев, потерей идеологии, старые ценности перестали действовать, а новые не успели сформироваться. Результатом стало целое поколение, выросшее в этот трудный переходный период. Сегодняшнее российское общество сталкивается с различными проблемами, вызванными этими перестроениями социально-культурных ориентиров и ценностей, существенными изменениями в политической сфере, стремлениями иностранных государственных органов поддержать деструктивные проявления на территории Российской Федерации в целях дестабилизации обстановки в стране.

Большинство существующих проблем в российском государстве, как и в любом другом, возникают, как естественно, так и искусственно. Это и возрастающий уровень организованной преступности, коррупция во всех ее проявлениях на различных уровнях власти, бандитизм, разведывательная и иная подрывная деятельности иностранных спецслужб и организаций, а также отдельных граждан, ставящих своей целью нанесение непосредственного ущерба безопасности Российской Федерации и, конечно же, экстремистская деятельность. Являясь наиболее сложной проблемой, экстремизм уже давно вышел за пределы границ отдельных государств и представляет глобальную угрозу безопасности всего мирового сообщества.

В настоящее время экстремизм характеризуется многообразием форм проявления, неоднородным составом экстремистских организаций, а также стремлением радикальных сообществ достигать свои цели путем воздействия на та-

кие общественно значимые сферы, как политика и религия. Не редко политический экстремизм подкрепляется извне. На государства, у которых имеются определенные проблемы в социально-культурной, экономической и иных сферах, оказывается непосредственное внешнее деструктивное влияние иностранных спецслужб и организаций в целях дестабилизации ситуации в стране. Особенно это хорошо видно на примере стран, входивших в состав бывшего Советского Союза. События в Республике Беларусь показывают, что влияние третьих сил способно привести к длительной дестабилизации обстановки в стране. «Проблемная» ситуация после выборов, связанная с легитимностью действующего президента, под воздействием существующих экстремистских организаций на территории страны, ставящие своей целью продвижение конкретных экстремистских идей, в том числе в политические массы, а также организаций, стремящиеся приватизировать власть всеми возможными методами, привела к массовым беспорядкам. При этом эти силы получили значительную поддержку из «демократических» стран под эгидой демократизации общества. Был подготовлен мощный плацдарм для деструктивной деятельности экстремистов.

Современное понятие экстремистских явлений может определяться поразному, в зависимости от того, кому принадлежит та или иная точка зрения: ученым, политическим деятелям или потенциальным экстремистам. На определение может оказывать влияние множество факторов, таких как недемократический характер политической системы, преобладающая политическая культура, система ценностей, идеология, политические цели, личные характеристики и опыт, этноцентризм и многие другие. Экстремизм в терминах терроризма, расизма, ксенофобии, межэтнической и межрелигиозной ненависти, левого или правого политического радикализма и религиозного фундаментализма, по сути, является политическим термином, определяющим те действия, которые морально, идеологически или политически не соответствуют правовым нормам государства, которые полностью нетерпимы по отношению к другим и отвергают демократию как средство управления и, наконец, отрицают существующий общественный строй. Данное определения имеет существенные недостатки, это связано, прежде всего с тем, что, во-первых, оно не является достаточно точным с юридической точки зрения, чтобы быть эффективным, а во-вторых, оно может быть философским, социологическим, психологическим и тем более политически некорректным. В связи с этим актуальность вопроса определения понятие экстремизма сохраняется и по сей день.

Отношение преступлений экстремистской направленности к общему количеству преступлений, совершаемых в Российской Федерации не велико. Но не обращать на такой вид правонарушений нельзя, так как любое такое преступление получает моментально огромный общественный резонанс, и может привести к быстрой дестабилизации ситуации, как в конкретном регионе, так и в стране в целом.

Развитие информационно-телекоммуникационных технологий привело к тому, что появляется все большее количество активных пользователей сети Интернет. Если раньше, десять-двадцать лет назад, активными пользователями сети были в основном жители больших городов, при этом они были достаточно образованы, то сегодня для получения доступа к сети и работы в ней не нужно никаких дополнительных знаний, опыта, проводить время в сети начинают с раннего детства. Условия для выхода в Интернет появились фактически везде, и чтобы работать там, достаточно иметь смартфон, планшет или компьютер, т. е. любое устройство, предоставляющее доступ к сети. Представители экстремистских организаций также оценили удобство и простоту использования контента в сети, они заняли свою нишу, размещая материалы, возбуждающие ненависть и вражду по признакам пола, расовой, национальной, языковой, религиозной принадлежности или принадлежности к какой-либо социальной группе. Через Интернет происходит распространение призывов к насильственным действиям, проведению несогласованных акций, организации массовых беспорядков и совершении террористических актов.

Органы государственной власти ведут активную борьбу по данному направлению. Делается очень многое для того, чтобы противоправный контент, содержащий идеи экстремистской направленности, выявлялся, блокировался и удалялся. Но все удалить из сети Интернет невозможно, если учесть, что члены экстремистских преступных организаций также меняют свою тактику, приспосабливаясь к меняющимся условиям. Блокирование, удаление противоправного контента, привело к перемещению его в закрытую часть сети.

Последние годы широкое распространение получили различные социальные сети. Социальные сети предназначены для общения пользователей в виртуальной среде. Они позволяют людям во всем мире находить единомышленников, делиться мнениями, впечатлениями, мыслями, стирая между ними границы. С одной стороны, это превосходно, но с другой стороны виртуальные социальные сети часто используются как информационный ресурс для формирования экстремистских настроений, а также, как инструмент для привлечения граждан Российской Федерации к преступной деятельности. Наиболее активно используют социальные сети вербовщики запрещенной в России террористической организации ИГИЛ. Объектами и жертвами таких вербовок часто становятся учащаяся молодежь, а также представители маргинальных групп общества. Именно они наиболее уязвимы и подвержены формированию радикальных взглядов и убеждений.

Одним из основных направлений использования интернета террористами является пропагандистская деятельность. Обычно пропагандистские материалы представляются в форме мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, а также рекламу террористической деятельности. К ним относятся электронные сообщения, презента-

ции, журналы, теоретические работы, аудио- и видеофайлы, а также компьютерные или мобильные игры, разрабатываемые террористическими организациями. Противоправность таких материалов обуславливается, прежде всего, тем, что они наносят ущерб защите национальной безопасности, а также такие сообщения, имеют своей целью и способы побудить людей к актам насилия в отношении отдельных лиц или определенных групп лиц. При этом можно отметить, что интернет в отличие от привычных средств массовой информации или традиционных средств агитации обладает огромной областью охвата. Традиционные СМИ ограничены тиражом, телевидение – областью вещания, привычная агитация – аудиторией, с которой происходит непосредственный контакт, то в социальных сетях таких ограничений не существует. Яркий, привлекательный контент может привлечь внимание миллионов людей. Охват аудитории значительно увеличивается при незначительных издержках со стороны разработчиков такого материала, и если отдача будет составлять даже несколько человек – это уже успех для участников террористической, экстремистской деятельности. Другой особенностью распространения противоправных материалов через Интернет, социальные сети связан с тем, что нет непосредственного контакта между представителями террористических организаций и потенциальными сторонниками, все общение происходит дистанционно. Пользователи сети могут изначальной даже не подозревать, что в отношении них проводятся определенные вербовочные мероприятия. Зачастую все начинается с обычного общения, переписки, где между прочим время от времени проскальзывают мысли, например, о превосходстве отдельной религии, расы, национальности и т. д., появляются тезисы, поддерживающие насилие. Интернет-пропаганда также может включать в себя и видеоигры, имитирующие акты терроризма и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста.

Основная угроза, которую несет с собой террористическая и экстремистская пропагандистская деятельность, связана с тем, как она используется и в каких целях распространяется. Они могут быть приспособлены для воздействия, в частности, на потенциальных или реальных сторонников, или противников той или иной организации или общих экстремистских воззрений, на прямых или косвенных жертв террористических актов или на международное сообщество в целом. Ориентированная на потенциальных или реальных сторонников пропаганда может быть направлена на вербовку, радикализацию и подстрекательство к терроризму путем рассылки сообщений с выражением чувств гордости, удовлетворения от успехов и преданности экстремистским целям. Целевая аудитория может включать как тех, кто непосредственно видит эти материалы, так и тех, кто окажется под воздействием потенциальной огласки, которую такие материалы приобретают.

Таким образом, обобщая вышеизложенное, следует отметить, что с развитием интернет-технологий представители экстремистских и террористических сообществ получили возможность осуществлять пропаганду экстремистской идеологии дистанционно. Такой подход имеет ряд преимуществ: широкий охват аудитории; высокая скорость и простота распространения информации; анонимное размещение материала; анонимная организация Интернет-ресурсов ведения пропаганды.

Список литературы

1. Федеральный закон Российской Федерации от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации. 2002. № 30. С. 230.

2. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_353838/. Режим доступа: по расписанию.

3. Беликов С. В. Антифа. Молодежный экстремизм в России. М. : Эксмо, 2012.

4. Андреев М. В. Основы теории национальной безопасности : учебник. Казань : Центр инновационных технологий, 2012.

Крылова С. В.[1]*,*
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Е. Н.[2]*,*
доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ПРИЧИНЫ УЯЗВИМОСТИ УЧЕБНЫХ ЗАВЕДЕНИЙ ПЕРЕД СОВРЕМЕННЫМИ ТЕРРОРИСТИЧЕСКИМИ УГРОЗАМИ

Согласно п. 17 статьи 12 Закона «О полиции» на полицию возлагаются обязанности по участию в мероприятиях по противодействию терроризму, а также по защите объектов и мест массового пребывания граждан от террористических посягательств, по проведению экспертной оценки состояния антитеррористической защищенности и безопасности объектов.

В последние годы мы все чаще слышим о совершенных или готовящихся преступлениях террористической направленности в учебных заведениях. Ужасные события в Казани и Керчи показали, что от безопасности территории учебного заведения напрямую зависят жизнь детей, подростков, учителей. Отличительной особенностью последних случаев является то, что все они были совершены молодыми людьми.

Подростки на сегодня являются наиболее уязвимой категорией, так как в их возрасте, в период взросления, выстраивается процесс социального сравнения от реального до идеального.

Количество преступлений, совершенных молодыми людьми постоянно увеличивается. При этом преступность характеризуется своими специфическими признаками, связанными, прежде всего, с возрастом, уровнем психического и общеобразовательного развития, условиями жизни, увлечениями, и воспитания в семье, социальной и информационно-телекоммуникационной средой и многими другими факторами современной жизни.

Подростки во все времена были агрессивными. Это свойство присуще подростковой психики, физиологии, и от этого никуда не деться. Молодой человек не понимает, чего он хочет, что ему в жизни надо. При этом он остро нуждается в поддержке, опоре, сочувствии родителей, учителей, взрослых, а ничего из этого в нужный момент может и не быть. В этом случае, в последние годы сеть Интернет может оказаться самым близким и доступным помощником, заполняя пустоту внутри подростка. В сети Интернет молодой человек может найти все, что ему требуется в данный момент, получить всю необходимую информацию. Зачастую они проводят там большую часть своего времени, бесконтрольно перемещаясь по сети.

Деструктивные ARG, кибербуллинг, онлайн-груминг. Многие взрослые даже не знают этих терминов и того, что за ними скрывается. А это только несколько из наиболее актуальных информационных угроз, с которыми молодежь может столкнуться в глобальной сети.

Психологи утверждают, что активное использование социальных сетей негативно сказывается на самочувствии и самооценке молодых людей. Сегодняшние подростки растут во время экономического, экологического, социально-психологического кризисов, да еще и во время COVID-19, и это отражается на их жизни. Подрастающее поколение предпочитает переписываться и разговаривать с друзьями, близкими и незнакомыми им людьми в онлайн-формате, и учить их необходимо правилам поведения в виртуальном пространстве. Реальное очное общение повсеместно заменяется на виртуальное.

У несовершеннолетних происходит дереализация. Психиатрический термин, который обозначает, что, постоянно находясь в виртуальном мире социальных сетей или игр, молодой человек теряет связь с реальностью и начинает воспринимать законы игры как законы реального мира. В игре можно умереть, а затем воскреснуть. Подросток перестает видеть грань между выдуманным миром и настоящей реальностью. Жестокие стрелялки, насилие, драки, боевики, постепенно становятся нормой обыденной жизни, приводя к жестокости, насилию, убийствам в обычной жизни и это уже факт.

В последние годы в России появилась и обострилась проблема так называемого скулшутинга[1]. Трагедии с нападениями в учебных заведениях стали повторяться с тревожной регулярностью.

Практически каждый день в одной из школ или детских садов охранник вмешивается в ту или иную ситуацию, которая иначе могла бы представлять опасность для жизни и здоровья окружающих. За 2020 год было пресечено более ста попыток проникновения на объекты образования. А это не просто случайно забредшие люди, которые не представляют опасности. Эти лица в состоянии алкогольного и наркотического опьянения, психически неуравновешенные[5].

Статистки показывает, что все «школьные стрелки» обычно заранее говорили, что готовят преступление. Они всегда действуют отнюдь не беспорядочно, всегда есть закономерность и причина их действий. Если вспомнить казанского стрелка, то он тоже заявлял в сети, что всех ненавидит и хочет убить. И вымещение обиды произошло. В таких ситуациях почти все жертвы случайны, стреляют в кого попадется. Все такие преступления объединяет то, что это истории про демонстративность, про неполноценность и попытку доказать, что я «крутой».

Почему же происходят такие события, если злоумышленник часто даже не скрывает свои намерения. Прежде всего, для нашей страны такие преступления являются «дикими», нам очень трудно представить, что кто-то может обидеть ребенка, подростка, поэтому они всегда для нас носят неожиданный характер. Поэтому часто учебные заведения просто к такой опасности не готовы.

---

[1] Скулшутинг (от англ. *school shooting* – «школьная стрельба») – применение вооруженного насилия на территории образовательных учреждений (главным образом к учащимся), очень часто перерастающее в массовые убийства.

На различных занятиях по обеспечению безопасности жизнедеятельности обсуждаются вопросы и рассматриваются ситуации с возникновением пожара, обнаружением взрывного устройства, оказанием первой медицинской помощи и т. д., но фактически никогда не проводятся учения, связанные с появлением, такого «стрелка». Большое количество жертв таких случаев связано не только с непосредственным контактом окружающих с преступником, но и с их неправильным поведением, не знанием как вести себя в конкретной ситуации. Несовершеннолетние, много проводя времени за разными играми, часто переносят виртуальные правила в реальную жизнь. Оказавшись в экстремальной ситуации, они зачастую думают, что можно легко спрыгнуть со второго, третьего этажа, подняться и побежать дальше, и при этом не погибнуть и не получить травмы. В данном случае существует только три стратегии выживания: прятаться, убегать, сражаться. Если нет возможности убежать, необходимо затаиться и не привлекать к себе внимание, никак не отвечать на агрессию, потому что человек с оружием ищет эту агрессию.

Следующей причиной таких событий является недостаточная защищенность учебных заведений. Еще двадцать пять лет назад никто не думал об охране учебных заведений от террористических или иных угроз. Для обеспечения безопасности материальных ценностей привлекались самые обычные сторожа. А сегодня, начиная с детского сада и заканчивая высшем учебным заведением, все охраняются частными охранными организациями. И здесь возникает вопрос связанный с качеством оказания услуг, уровнем квалификации охранников, которые находясь на посту, должны оценивать обстановку с точки зрения безопасности, подмечать странности в поведении несовершеннолетних, подозрительных людей рядом с учебным заведением.

Подросток, задумавший прийти в школу с оружием, ведет себя не так, как его сверстник, идущий на учебу. Есть выбор одежды, характерный для так называемых «колумбайнеров», определенные особенности поведения, он не придет вместе с основным потоком, он будет среди опоздавших, как это случилось в Казани.

Еще одной отличительной особенностью все таких событий стало то, что все происходили по вине молодых людей, имеющих отношение к этому учебному заведению, чаще всего учившихся в нем и прекрасно знавших расположение помещений, систему организации охраны, а также все имеющиеся в ней недостатки.

Для решения вопроса обеспечения безопасности учебных заведений, недостаточно только вкладываться в обеспечение их физической защищенности. В конце концов, никто не хочет, чтобы дети, подростки учились в «непреступной крепости», все хотят, чтобы на территории учебного заведения они были в безопасности. Поэтому необходимо особое внимание уделять подросткам, которые потенциально могут встать на путь преступления. Для этого необходимо производить мониторинг социальных сетей, где они проводят значительное количество времени. Ведь именно ради привлечения внимания в социальных сетях психически неуравновешенные молодые люди пишут сообщение о том, что собираются совершить террористические акты. И здесь их можно вычислить по

ключевым словам – тексты они используют понятные для всех: «взорвать», «застрелить», «убить», «распылить газ». Это достаточно сложная система, но она возможна. Возможно, не все социальные сети надо отслеживать, а только наиболее популярные в молодежной среде, такие как Telegram, WhatsApp, Instagram.

Информация, размещаемая на форумах, в социальных сетях должна контролироваться, что необходимо в целях пресечения попыток размещения недостоверной информации различными радикальными лицами, стремящихся вовлечь подростков в преступную деятельность, так как очень часто молодой человек не сам «додумался» до совершения преступления, а ему помогли.

Необходимо восстанавливать систему воспитательной работы, чтобы делами молодых людей кто-то действительно интересовался, они кому-то были нужны, а не оставались один на один с Интернетом со всеми своими проблемами.

Со своей стороны, правоохранительные органы проводят значительное количество совместных мероприятий, направленных на противодействие террористических проявлений и профилактике терроризма. В средствах массовой информации периодически мелькает информация о предотвращении очередной трагедии, но в данном случае даже один произошедший инцидент – это много. Поэтому необходимо продолжать совершенствовать механизмы взаимодействия и совместного решения наиболее важных вопросов, связанных с террористической защищенностью на различных направлениях, в том числе на устранение причин и условий, способствующих совершению преступлений в учебных заведениях, совершенствованию системы профилактической, воспитательной работы.

Список литературы

1. Приказ Минобрнауки России от 25 апреля 2019 г. № 247 «Об организации работы в Министерстве науки и высшего образования Российской Федерации по обеспечению условий для формирования у молодежи гражданской позиции, противодействия идеологии терроризма и экстремизма» // СПС «КонсультантПлюс». URL: http://www.consultant.ru. Режим доступа: через коммерческую версию (дата обращения: 15.11.2021).

2. Сидненко Г. Ф. Информационное противодействие терроризму: политологический аспект // URL: http://nac.gov.ru/sites/default/files/protivodeystvie_terrorizmu_ 0.pdf (дата обращения: 15.11.2021).

3. Чернышов Г. Н. Проблемы подросткового возраста. http://garant48.ru/regionalnye-stati/obshhaya-psixopatologiya-podrostkovogo-vozrasta-–-problemy-i-resheniya (дата обращения: 15.11.2021).

4. Влияние интернета на психику подростков // URL: https://www.google.ru/ amp/ipsyholog.ru/vliyanie-interneta-na-psihiku-podrostkov/amp (дата обращения: 15.11.2021).

5. Как сегодня охраняют школы в Москве? // Полиция и гражданское общество. 2021. № 18 (9764).

Шарапа Е. И.[1]*,*
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Е. Н.[2]*,*
доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМА РАСПРОСТРАНЕНИЯ ДЕСТРУКТИВНОГО КОНТЕНТА ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В СОЦИАЛЬНЫХ СЕТЯХ ЧЕРЕЗ ПОДРОСТКОВУЮ АУДИТОРИЮ

С каждым годом граждан, активно пользующихся сетью «Интернет» в России, становится все больше, помимо этого в последние время бурное развитие получили различные социальные сети такие как: «Facebook», «Twitter», «ВКонтакте», «Одноклассники», «Мой Мир». При этом информационные материалы, размещенные в сети, могут иметь совершенно разный характер, от безобидных фотографий и материалов, до изображений порнографической, экстремистской, террористической, суицидальной направленности. В рамках данной работы нас интересует контент, имеющий террористическую направленность.

Проблема деструктивного контента террористической направленности в сети «Интернет» является в настоящее время очень актуальной. За последнее десятилетие количество негативных материалов, размещаемых на разнообразных площадках и ресурсах в глобальной сети, значительно увеличилось, и это становится действительно серьезной проблемой для социума. Следует также отметить, что целевой аудиторией, адресатами такого деструктивного контента в сети Интернет чаще всего выступают подростки. На это есть несколько причин:

1. Сознание подростка полностью не сформировано, в связи с этим на молодежь проще психологически воздействовать, навязать определенную политическую, религиозную идею.

2. Основная часть пользователей в социальных сетях – лица, подросткового возраста.

При этом, рассматривая проблему распространения контента террористической направленности, не стоит забывать и о том, что социальные сети нередко используются деятелями других стран как эффективный инструмент дестабилизации внутриполитической и социальной целостности нашей страны. Не случайно в п. 43 Указа Президента Российской Федерации от 31 декабря 2015 г.

№ 683 «О Стратегии национальной безопасности Российской Федерации» к основным угрозам национальной безопасности государства отнесена деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе».

Продвижение террористических идеологий является одним из самых опасных направлений деструктивного контента для общества и государства. Терроризм – политика, которая основывается на достижении определенных целей (политических, экономических, идеологических и других) с помощью насилия. Продвижение террористических идеологий – колоссальная опасность для общества. Вследствие этого, Правительство Российской Федерации и органы исполнительной власти непрерывно анализируют данную проблему, разрабатывая варианты ее решения.

Одно из основных направлений, в котором активно действуют террористы, связано с пропагандой, популяризацией своей деятельности. Чаще всего это осуществляется с помощью поощрений насилия, при этом такая деятельность является конкретно направленной (целью могут стать потенциальные сторонники или противники какой-либо организации), а также часто содержит политическую идеологию. Используя такой деструктивный контент террористы стремятся подорвать социальные ценности и устрашить определенные группы населения. Террористы тщательно подбирают группу для будущей работы и вербовки. Критериями отбора может стать грамотность, вероисповедание, политические интересы, возраст и другие параметры. Наиболее ярким примером такой вербовки является Варвара Караулова. По ее словам, вербовка произошла с помощью социальной сети «ВКонтакте». В данной социальной сети она познакомилась с Владом, которого в реальной жизни зовут Айрат Саматов. После продолжительного общения с ним, Варвара Караулова поняла, что влюбилась в молодого человека, она разделяла его взгляды, приняла ислам. Также Караулова просила Саматова взять ее в жены и увезти в Сирию, где Саматов принимал участие в военных действиях как сторонник Исламского Государства, которое запрещено в России.

За последние двадцать пять лет появилось направление террористической деятельности, связанное с нападением на учебные заведения, и получившее название «колумбайн» по месту первого такого происшествия. Первое событие убийства в школе подростками произошло в 1999 году в школе «Колумбайн» штата Колорадо, США. Двое подростков Эрик Харрис и Дилан Климборд на своем персональном сайте размещали разработки уровней компьютерной игры «Doom». Кроме разработок Эрик Харрис в блоге появлялись материалы с деструктивным юмором о школе, учителях и родителях, затем он уже стал активно освещать тематику ненависти к обществу, а перед совершением массового

убийства там появилась информация о способах изготовления взрывчатых устройств. Таким образом, мы можем говорить о том, что подобный деструктивный паблик подтверждает колоссальное содержание негативных последствий, которые может принести социуму юмор в рамках разрушительной коммуникации.

При анализе проблемы воздействия контента террористической направленности на подростков необходимо помнить, что подростки с психологической точки зрения являются самой уязвимой социальной группой, которая чаще всего подвергается психологическому манипулированию и насилию. Это происходит потому, что подросток в силу своего возраста начинает отдаляться от родителей, но при этом не имеет свои внутренние жизненные установки, ценности, помогающие противостоять различного рода угрозам, в том числе и информационным, в реальном и виртуальном мире.

Таким образом, получается, что при столкновении с жизненными трудностями, которые для взрослого человека не покажутся значимыми, подросток уходит в депрессию, не зная, как поступать в данной ситуации, путаясь в потоке своих мыслей, зачастую, не имея поддержки от родных, друзей, учителей. В подобном психологическом состоянии подростку кажется, что выхода из плачевной ситуации нет. За советом, общением молодые люди идут в социальные сети, там всегда найдется кто-то, кто посоветует, выслушает. В социальные сети подросток идет за одобрением, поднятием своего социального статуса. При этом социальное одобрение выражается с помощью своеобразных количественных показателей: лайки, репосты, комментарии под постами. И для получения такого признания, подростки демонстрируют то, что является актуальным, признанным в сети, даже если оно очевидно обладает негативным и токсичным содержанием. Такие образом, уровень критики для последующей фильтрации контента в социальных сетях у подростков значительно снижен.

Деструктивный контент появляется в аккаунтах (группах), которые имеют больше число подписчиков. Любая информация, которую размещает такая группа в социальной сети, мгновенно одобряется пользователями и начинает распространяться, а так как членами таких сообществ в основном являются молодые люди, то такой контент распространяется как раз среди самой незащищенной категории пользователей, принося максимальный вред.

Манипуляция подростковым сознанием и поведением может происходить с помощью навязывания определенного авторитета, который якобы разбирается в том, как нужно поступать. Навязывание подобного значащего мнения происходит постепенно: вначале подросток видит группу сети Интернет с соответствующим контентом, манипуляторы привлекают его путем «доброжелательной обстановки», которой свойственны понимание, одобрение, уникальная исключительность ее членов, только подобное сообщество имеет правильные жизненные установки. Затем в данной виртуальной группе с помощью определенного

персонажа или авторитета подростку оказывают внимание в его индивидуальных проблемах, как правило, психологического содержания. Таким образом, у подростка появляется авторитет, которого он готов слушать и выполнять практические любые его команды.

Деструктивный контент распространяется чаще всего с помощью негативной информации. Как правило, подобного рода данные являются глобальными и вызывают сильные эмоции страха и интереса подростковой аудитории. Среди цели распространения контента токсичного содержания можно выделить следующие:

1. Оказывать с помощью деструктивного контента сети Интернет влияние на подростка для того, чтобы он медленнее развивался в моральном, психологическом, умственном направлениях.

2. Формировать образ успешного человека среди подростков с целью выделить себя среди других.

3. Стимулировать бессмысленное потребление и пагубные привычки в маркетинговых целях.

4. Разрушать общественные ценности.

5. Формировать процессы развития и воспитания подростков по определенным стандартам.

Таким образом, под воздействием деструктивного контента в сети «Интернет» подростки лишаются возможности взвешивать и принимать обдуманные решения, разрушаются базовые ценности и нормы морали, отрицается ответственность, ослабевают аксиологические авторитеты, ярко выражается стремление к разрушению.

В заключении отметим, что для борьбы с развитием и распространением деструктивного контента террористической направленности в сети «Интернет», целесообразно действовать по нескольким направлениям:

1. Организационные усилия различных ведомств. Для эффективной борьбы с данной проблемой следует привлекать к совместной работе различные ведомства.

2. Продолжение и наращивание оборотов ведения тщательной и непрерывной работы с медиа-контентом в социальных сетях и СМИ, расширение возможностей для быстрого поиска деструктивного контента, иных подобных информационных угроз, которые с большой скоростью набирают социальную активность.

3. Совершенствование нормативно-правового регулирования правоотношений в соответствующей сфере. В данном случае, речь идет о создании свода законов, которые будут регулировать ответственность за распространение ментальных вирусов, деструктивного контента и т.д.

4. Проводить просветительскую и агитационную работу среди подростков, в частности о признаках и вреде деструктивного контента в сети «Интернет», о

возможных последствиях ознакомления с содержанием и целях, преследуемых его создателями.

5. Усилить работу школьных психологов среди подростков, создать атмосферу доверия для реализации в дальнейшем помощи в подобных ситуациях.

Список литературы

1. Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_108808/.

2. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_191669/.

3. Новиков Д. А. Социальные сети и деструктивный контент. М. : Горяча линия-Телеком, 2020. 75 с.

Крупинская С. Р.[1]**,**
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Таранина Е. И.[2]**,**
преподаватель кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

СТАТИСТИЧЕСКОЕ ИЗМЕРЕНИЕ ПРЕСТУПНОСТИ В СФЕРЕ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

Согласно Концепции общественной безопасности в Российской Федерации [1] приоритетным направлением обеспечения общественной безопасности в нашей стране является противодействие[3] преступлениям экстремистского и террористического характера. Масштабность распространения социально-негативного явления рассматриваемого вида потребовала разработки на государственном уровне комплекса мер по противодействию экстремисткой деятельности. В этой связи была разработана и принята Стратегия противодействия экстремизму в Российской Федерации до 2025 года [2], в которой констатируется вовлечение лиц посредством информационно-телекоммуникационной сети «Интернет» в состав организаций, деятельность которых запрещена на территории нашей страны, а также распространение призывов к насильственной деятельности.

Наблюдается, что данные формы федерального статистического наблюдения демонстрируют незначительное снижение в относительных и абсолютных показателях выявления лиц, совершивших преступления экстремистского характера.

Таблица 1

Динамика количества выявленных лиц [4] за совершение преступлений экстремистского характера в Российской Федерации в 2018-2020 гг.

	Годы		
	2018	2019	2020
Экстремисткой направленности	894	445	664
Всего выявлено лиц	931107	884661	852506
Удельный вес лиц выявленных лиц за совершение преступлений экстремисткой направленности, %	0,096	0,050	0,077

[1] © Крупинская С. Р., 2021.
[2] © Таранина Е. И., 2021.
[3] Включая предупреждение, выявление пресечение преступлений рассматриваемых видов.

Анализ данных в табл. 1 в трехлетней ретроспективе и по итогам 2020 г., показал, что удельный вес лиц, выявленных за совершение преступлений экстремистской направленности составляет менее 1 %.

Подавляющее большинство лиц, выявленных за совершение рассматриваемых преступлений – граждане Российской Федерации: 2018 – 859 лиц (96,08 %), 2019 – 437 лиц (98,2 %), 2020 – 633 лица (95,33 %). Доля женщин, совершающих преступления экстремистского характера также незначительна, и в среднем составляет 54 человека.

Фиксируется стабильный рост преступлений в сфере информационных технологий. Так, например, в 2020 г. было зарегистрировано 504 966 преступлений (прирост к 2019 году + 73 %). Увеличение числа зарегистрированных преступлений рассматриваемого вида наблюдается во всех субъектах Российской Федерации (табл. 2).

Таблица 2

Динамика зарегистрированных преступлений [5] в сфере информационных технологий по Федеральным округам Российской Федерации

Федеральный округ	Зарегистрировано преступлений в 2020 году	Темп прироста, %
Центральный ФО	123002	92,4
Северо-Западный ФО	58698	124,5
Северо-Кавказский ФО	14526	68,6
Южный ФО	50677	70,9
Приволжский ФО	109178	56,6
Уральский ФО	51004	52,9
Сибирский ФО	69103	67,4
Дальневосточный ФО	28403	62,5

В структуре преступлений экстремисткой и террористической направленности, совершенных с использованием информационно-телекоммуникационных технологий, преобладают такие составы:

1. Статья 205.1. Содействие террористической деятельности – 260 преступлений.

2. Статья 205.2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма – 350 преступлений.

3. Статья 207. Заведомо ложное сообщение об акте терроризма – 2153 преступления.

4. Статья 280. Публичные призывы к осуществления экстремисткой деятельности – 429 преступлений.

Сохраняется стабильность пополнения Федерального списка экстремистских материалов [6], в состав которых входят:

1. Статьи.
2. Листовки.
3. Брошюры.
4. Книги.
5. Номера газет и журналов.
6. Аудио- и видеоматериал.

Так, например, за 9 месяцев 2021 года 136 материалов были признаны экстремистскими на основании судебных решений. По состоянию на июль 2021 года указанный список содержит 5178 позиций, при этом исключена возможность повторений сведений. Анализ имеющихся данных показал, что такие материалы преимущественно распространяются при помощи информационно-телекоммуникационной сети Интернет, то есть в открытом доступе, в формах, перечисленных авторами выше.

Тенденции увеличения абсолютных значений зарегистрированных преступлений в сфере терроризма и экстремизма коррелируется с общероссийской тенденцией увеличения преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Адаптация преступности к происходящим в социуме изменениям носит поступательный характер: изученные статистические сведения демонстрируют смещение вектора преступности в сферу высоких технологий и, как следствие, применяются иные, непривычные для нецифрового общества способы осуществления противоправной активности.

Список литературы

1. Концепция общественной безопасности в Российской Федерации (утв. Президентом Российской Федерации 14.11.2013 № Пр-2685). // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_154602/ (дата обращения 20.11.2021).

2. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом Российской Федерации 28.11.2014 № Пр-2753) // СПС «КонсультантПлюс». URL:http://www.consultant.ru/document/cons_doc_-LAW_194160/ (дата обращения 20.11.2021).

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_-law_10699/ (дата обращения: 20.11.2021).

4. Сведения ГИАЦ МВД России. Форма 492, книга 1. Сводный отчет по России. Сведения о лицах, совершивших преступления.

5. Сведения ГИАЦ МВД России. Форма 494, книга 31. Сборник по России. Раздел 11. Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации.

6. Федеральный список экстремистских материалов // URL: https://minjust.gov.ru/ru/extremist-materials/?page=1&q=2021 (дата обращения: 19.11.2021).

Маклаков Е. Д.[1]**,**
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Овчинский А. С.,***
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

ЦИФРОВЫЕ ПЛАТФОРМЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННЫХ СФЕРАХ

Развитие коммуникационных технологий, стремительная цифровизация всех сторон жизни все более явственно фокусирует угрозы криминализации, терроризма и экстремизма на информационные сферы.

Можно по-разному раскрывать понятие информационных сфер. Принято считать, что это сферы производства и оборота информационных продуктов, отношений субъектов на рынке информационных и коммуникационных услуг и так далее.

Но можно взглянуть на информационные сферы значительно шире и тогда станет ясно, что они охватывают отношения между людьми, сообществами, народами, все те отношения, которые построены на информационных взаимодействиях. Важно, что информационные сферы не только отражают, но и образуют те идеальные миры (а следуя популярным кинематографическим образам, те информационные матрицы), в которых протекает вся жизнь людей, будь-то семья, учеба, работа, служба, досуг.

Как правило, люди взаимодействуют сознательно. Но именно в сознании возникают модели прошлого, настоящего и будущего. Главное же, именно в сознании человека рождается то, что становится информацией. Она может быть реакцией на внешние воздействия или внутренние побуждения. Она является функцией целевой интерпретации получаемых сообщений и сигналов. Важно, что эта реактивная информация создает и накапливает потенциалы энергии, желаний и стремлений. Разрядка этих потенциалов социально психологической энергии приводит к действиям и поступкам [1].

Здесь то и кроются механизмы зарождения, накопления и реализации как позитивных, конструктивных, так и негативных, деструктивных проявлений активности отдельных личностей или организованных сообществ. Как результат накопления и разрядки энергоинформационных потенциалов мы имеем череду событий, среди которых террористические акты, экстремистские выступления, корыстные преступления… Еще мыслители Древней Греции отмечали, что явления, созревая в потенции, актуализируются в реальности.

---

[1]

Говоря о безопасности информационных сфер, о противодействии терроризму и экстремизму, выкристаллизовывается задача: не давать социальной деструкции зарождаться и созревать в информационных сферах. Решаться эта задача может на основе современных и перспективных технологий контроля, воздействий и управления социальными процессами.

В условиях цифровизации, обеспечение безопасности информационных сфер видится в создании функциональных цифровых платформ, накапливающих необходимые энергоинформационные потенциалы и цифровых инструментальных платформ, направляющих потоки социальной психологической энергии в нужное русло [2].

Цифровые платформы сегодня – это весьма емкое понятие, используемое в коммерции, логистике, военном деле, государственном управлении. Можно встретить описание программных, инфраструктурных, отраслевых платформ. Так, эксперты-футурологи представляют государство уже недалекого будущего в виде цифровой платформы, включающей алгоритмы автоматического управления экономикой, финансами, правовой системой, социальной сферой, внутренней и внешней безопасностью… на основе возможностей искусственного интеллекта.

Реально же, можно говорить о закрытых цифровых платформах, настроенных на решение внутренних корпоративных задач. Здесь просматриваются перспективы, скажем, цифровых платформ, оперативно-разыскной аналитики или оперативно-разыскной профилактики преступлений.

Однако, наибольшие возможности в управлении процессами декриминализации общественных отношений, в противодействии терроризму и экстремизму открывает создание открытых цифровых платформ. Открытые платформы наряду с алгоритмами накопления и обработки данных включают еще и коммуникационные серверы, построенные, например, по принципу социальных сетей.

Именно архитектура открытых цифровых платформ должна создать пространство для интерактивного общения, для формирования мировоззренческих позиций, идеологических установок, направленных на противодействие социальной деструкции. Коммуникационные алгоритмы открытых платформ должны включат механизмы целенаправленных воздействий на сознание людей, попадающих под влияние деструктивных идей, таких идей, которые побуждают к противоправным, насильственным действиям.

Эффективность функционирование открытых цифровых платформ противодействия терроризму и экстремизму может быть обеспечена опорой на мощный информационно-аналитический фундамент. Это могут быть условно закрытые блоки, включающие широкий спектр алгоритмов по сбору и обработке самых разнообразных данных, больших данных с применением систем искусственного интеллекта.

Этот закрытый фундамент цифровых платформ противодействия терроризму и экстремизму должен складываться из:

– алгоритмов поиска, обработки и накопления данных о лицах, в той или иной мере, вовлеченных в деструктивную деятельность, из оперативно-разыскных и профилактических информационных ресурсов;

– алгоритмов инициативной оперативно-разыскной аналитики, позволяющих на основании анализа ресурсов оперативно-разыскной информации выявлять и ранжировать лиц, представляющих угрозу безопасности, например, в ходе проведения тех или иных массовых мероприятий;

– алгоритмов предиктивной оперативно-разыскной аналитики, позволяющих предсказывать противоправные действия и поступки на основании совокупности цифровых данных о «клиентах», попадающих в поле зрения правоохранительных органов;

– алгоритмов актуальной аналитики, позволяющих на основании складывающейся криминальной обстановки в том или ином регионе прогнозировать время и место ожидаемых преступлений, возможных исполнителей и заказчиков.

Цифровые платформы должны включать алгоритмы лингвистического анализа, позволяющие выявлять и ранжировать угрозы, содержащиеся в экстремистском и террористическом контекстах, а также алгоритмы психологического анализа, позволяющие получать максимально информативные цифровые профили о лицах, представляющих оперативный интерес.

Алгоритмы обработки данных, обеспечивающие коммуникационные серверы открытых блоков, составляющих собственно архитектуру цифровых платформ противодействия терроризму и экстремизму должны быть настроены непосредственно на профилактику преступлений.

Основным инструментом должны стать адресные, целенаправленные информационно-психологические воздействия как на определенные реальные или виртуальные сообщества, так и на конкретных лиц с целью предупреждения, предотвращения и пресечения экстремистских выступлений, недопущения террористических актов.

Целью обработки ресурсной и фоновой оперативно-разыскной информации, т. е. накопленных, поступающих и циркулирующих в Интернет-коммуникациях и массмедиа-данных должны стать как проведение мероприятий по недопущению готовящихся преступлений, так и меры по криминологической профилактике, направленные на выявление и ликвидацию причин формирования криминальных потенциалов.

Основная функция открытых цифровых платформ противодействия терроризму и экстремизму – это информационные воздействия, включающие общесоциальную профилактику, а по существу формирование позитивного, патриотического жизнеутверждающего фона в массовом сознании, в информационных сферах.

Список литературы

1. Овчинский А. С., Борзунов К. К., Чеботарева С. О. Информационные координаты. Управление. Противоборство. Безопасность. М. : Горячая линия-Телеком, 2018.

2. Овчинский А. С. Цифровые платформы оперативно-разыскной профилактики преступлений // Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов. М. : Инфра-М, 2021.

Коломина А. С.[1]*,*
курсант факультет подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Атласов И. В.***[2]*,*
профессор кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор физико-математических наук, профессор

ОБ ЭФФЕКТИВНОСТИ РАБОТЫ ПРОГРАММЫ ПО ОБНАРУЖЕНИЮ ВИРУСОВ

В современном мире никто уже не представляют свою жизнь без технологий. Почти у каждого сегодня есть настольный персональный компьютер. Но с ростом технологий в нашей жизни происходит и рост вероятности угроз со стороны информационного воздействия. Многие даже не замечают, как злоумышленники получают личные данные пользователей персональных компьютеров. Большинство вирусов можно получить при скачивании с непроверенных сайтов, при подключении съемных накопителей, если на них изначально были вирусы и т. д. Итак, что же такого страшного в этих вирусах?

Компьютерные вирусы назвали в честь вирусов, которые существуют в мире. Это неклеточные инфекционные агенты, которые могут воспроизводиться только внутри клеток. Компьютерные же назвали так, потому что они внедряются в код других программ и наносят ущерб им. Такие вредоносные программы нацелены на кражу личных данных, уничтожения их, удаления файлов, ценной информации, вывод из строя программ, программно-аппаратных комплексов, нарушают работоспособность операционной системы и другое. Существует несколько классификаций компьютерных вирусов.

Классификация вирусов по способу заражения:

– резидентные, такие вирусы загружаются в память компьютера и начинают искать жертв постоянно, до выключения питания или завершения сеанса работы среды;

– нерезидентные, получив управление, такой вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту. сюда можно отнести скрипт-вирусы. они написаны на скрип-языках и заражают себе подобные программы, при этом они могут заражать и другие программы в которых также можно использовать скрипты.

Классификация вирусов по степени воздействия:

– безвредные, данные вирусы просто сокращают память на жестком диске, как таковой вред они не причиняют;

– неопасные вирусы похожие на безвредные, но они уменьшают память не только на дисках, но и в оперативной памяти, что может оказать воздействие на графические и звуковые эффекты;

– опасные, вирусы мешают работе компьютера, без удаления программ, файлов, данных;

– очень опасные, данная категория самая опасная, так как вирусы работают с целью за получения личной информации, удаление, искажение, модификация файлов, вывод из строя программ и так далее.

Классификация вирусов по способу маскировки:

– шифрованный вирус из названия следует, что вирус основанный на принципе шифрования, например, со случайным ключом и того, что шифр обычно не изменен, данный вирус отслеживается по сигнатуре шифратора;

– вирус-шифровальщик, этот тип вируса настроен на то, чтобы притворятся другими файлами, к примеру, пишется, что файл является документом (.doc), а на деле это исполняемый файл, при запуске которого начинает распространятся вирус;

– полиморфный вирус использует метаморфный шифратор[1] для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

Среда обитания – это то, где «живет» и находится вирус. Это может быть, как операционная система, так и приложения, файлы.

Классификация вирусов по среде обитания:

– файловые вирусы живут в файловых система ОС, они могут залезать в исполняемые файлы, создавать себе подобные вирусы, повторять сам файл, создавая двойника;

– загрузочные вирусы загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (master boot record), либо меняют указатель на активный boot-сектор;

– макро-вирусы многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий, макро-языки часто имеют сложную структуру и развитый набор команд, являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие;

– скрипт-вирусы это пример нерезидентных вирусов, основан на скриптовых языках (vbs, js, bat, php и т. д.).

---

[1] Метаморфизм – создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

Классификация вирусов по способу заражения файлов:

– перезаписывающие, смысл этого вируса заключается в том, чтобы перезаписывать данные файла, то есть данные изменяются без возможности восстановления, так как файл заполняется новой информацией, которую дает ей вирус;

– паразитические, этот вирус чем-то схож с перезаписывающим, но при этом он оставляет файл частично работоспособным;

– вирусы-компаньоны здесь вирус создает двойник, копию файла, который заражен, и он становится главным, то есть этот файл управляет процессами;

– вирусы-ссылки этот вирус является в прямом смысле ссылкой, которая отсылает ОС к своему коду и заставляет систему выполнить его, ссылка хранится в полях файловой системы;

– файловые черви не связывают свое присутствие с каким-либо выполняемым файлом, при размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии, например, install.exe или winstart.bat.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии.

Носителем же «живого» вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ- или LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ- или LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.

Рассмотрев небольшую классификацию вирусов можно сказать, что они умеют почти все, если не все, но как же с ними бороться. С каждым годом технологический прогресс идет все быстрей и быстрей, на сегодняшний день даже ученики средне образовательной школы могут написать вирус и загрузить в сеть. Существуют специальные сайты, обучающие создавать вирусы. Но как с ними борются по всему миру?

Самый простой и быстрый способ борьбы с вирусами, это программы по обнаружению вирусов, то есть антивирусные программы. Но помимо этого на многих операционных системах существуют встроенные защитники. К примеру операционные системы Windows поставляются со встроенным ПО для защиты от вирусов, шифровальщиков и эксплойтов. Приложение Защитник Windows обновляется по схеме, схожей с антивирусными программами, и не требует установки в систему, как это часто бывает с продуктами сторонних разработчиков. Большую часть времени его интерфейс скрыт от пользователя – нет всем надоевших значков в трее, защита работает прозрачно и автоматически блокирует потенциальные угрозы. Также существует модуль, предназначенный для

защиты от хакерских атак вроде несанкционированного удаленного подключения к компьютеру – брандмауэр.

Но что делать, если даже встроенного программного обеспечения не хватает для борьбы с вирусами? Решением становятся сторонние продукты, антивирусные программы, например, Kaspersky Internet Security, Avast Antivirus Professional, Dr.Web и другие. Оценкой наилучшей эффективности данных антивирусов занимаются по миру несколько крупных лабораторий, авторитет которых признается повсеместно. В случае России самым лучшим был признан Kaspersky Internet Security, получив оценку AAA во всех четырех квартальных тестах, проведенных SE Labs (Британская компания) для домашних продуктов. В рамках регулярных ежеквартальных исследований защитных решений для рабочих станций компания проводит два испытания: на качество защиты от угроз реального времени и на отсутствие ложных срабатываний.

Kaspersky Internet Security является хорошим антивирусом не только на Windows, но и на Android, macOS. Самое главное качество данного представителя в том, что компания не останавливается на достигнутом и постоянно двигается к новым вершинам, создавая и разрабатывая способы борьбы с вредоносными программами.

Таким образом, в статье была разобрана классификация вирусов, чем каждый из них опасен и отличается от других и приведены несколько способов борьбы с ними.

Список литературы

1. Компьютерный вирус // URL: https://www.tadviser.ru/index.php/ (дата обращения: 18.11.2021).

2. Тесты и награды независимых экспертов и решения «Лаборатории Касперского» // URL: https://www.kaspersky.ru/blog/kaspersky-awards-2020/30308/ (дата обращения: 20.11.2021).

3. Как правильно настроить Защитник Windows // URL: https:// timeweb.com/ru/community/articles/nastrojka-zashchitnika-windows-v-windows-10 (дата обращения: 15.11.2021).

4. Сравнение антивирусов по эффективности защиты от новейших вредоносных программ // URL: https://www.anti-malware.ru/comparisons/effect_antivirus (дата обращения: 15.11.2021).

Рахмонбердиев Б. Б.[1]*,*
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Зарипова Э. Р.****,*
доцент кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук

СИСТЕМА ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ, И РАБОТА С МОЛОДЕЖЬЮ

Во всем мире возникают проблемы терроризма и экстремизма. Развитие обстоятельств невозможно предсказать, поэтому важно провести все профилактические мероприятия, которые помогут не развивать терроризм на территории наших государств, создавать новые и укреплять уже существующие структуры по борьбе с терроризмом [1].

Организация договора коллективной безопасности (далее – ОДКБ) проводит специальные операции по борьбе с терроризмом, например, в 2019 году проведен комплекс профилактических мероприятий «Наемник» и «Прокси», проведено обучение антинаркотических кадров Азии на базе учебных заведений МВД России. Договор о коллективной безопасности был подписан в Узбекистане в 1992 г. главами Армении, России, Казахстана, Таджикистана и Узбекистана. Позже к ОДКБ присоединились Азербайджан, Белоруссия и Грузия. Последние миротворческие совместные учения «Нерушимое братство» проходили с 8 по 12 ноября 2021 г. в Российской Федерации в Республике Татарстан, где в ходе практических действий отрабатывались блокирование населенного пункта и штурм здания, занятого «террористами», выполнялись задачи в лагере беженцев, оказывалась первая помощь пострадавшим, сопровождались колонны с гуманитарным грузом. На учения были приглашены представители Монголии, Сербии, Узбекистана, Парламентской Ассамблеи ОДКБ Международного Комитета Красного Креста. На Организации договора коллективной безопасности большая ответственность, ведь кризисные ситуации в мире приходят как с западной, так и с восточной части мира.

На сегодняшний день в технологично развивающемся обществе все большей проблемой становится информационное воздействие на общество через социальные сети. Большое количество различных экстремистских группировок публикуют и вербуют разные слои населения через сообщества в социальных сетях. Размер угроз и глобальность ущерба от экстремистских и террористиче-

ских группировок, проплачиваемых наркотическим бизнесом, колоссален и приносит во все страны мира хаос и беспорядок.

Система противодействия имеет в каждой конкретной стране свои структуры, организации, особенности [2]. Органы национальной безопасности и Министерство внутренних дел выступает в качестве борца с группировками экстремистского характера в постсоветских странах. Существуют подразделения в структуре правоохранительных органов, которые в рамках своих полномочий выполняют управленческую роль в борьбе с терроризмом. Основными подразделениями являются ФСБ, МВД, Прокуратура, Следственный комитет России и некоторые другие службы. Внутри самих ведомств также прослеживается функциональное разделение. Правоохранительные органы применяют различные методологии для предотвращения негативных последствий терроризма. Постоянно проводится мониторинг социальных сетей, где после обнаружения мгновенно останавливается поток информации, связанный с пропагандой религиозного радикализма. Специальные подразделения в структурах органов внутренних дел ограничивают доступ к такому виду информации. Разрабатываются и развиваются сетевые методы выявления, оперативного отслеживания организации деструктивных информационных воздействий против безопасности государственного строя.

В социальных сетях пропаганда воздействует на самый молодой слой населения. Молодежь, попавшая под влияние, вовремя не осознает посыл происходящего. Первоначальным методом борьбы с попаданием под влияние – это поднятие моральных и духовных ценностей населения. В Республике Узбекистан в учебно-образовательную программу внедрены предметы, поднимающие морально-духовные ценности. Помимо школ и университетов, в Узбекистане есть специальный орган «Махаллинский комитет», основная задача которого – вовремя предотвратить схождение молодых с верного пути. Махаллинский комитет есть в каждом микрорайоне всей республики, он проводит вместе с представителями государственных органов беседы в школах и среди растущего поколения.

На открытии международной конференции летом 2021 года на территории Узбекистана в городе Ташкенте президент Узбекистана Мирзиеев Шавкат Миромонович предложил стратегию действий по борьбе с терроризмом, экстремизмом, а также транснациональной преступности, в том числе в киберпространстве. В качестве первого шага было предложено разработать совместный план участия в управлении ООН по наркотикам, а также разработать инфраструктуру транспортных перевозок. Узбекистан предложил организовать на его территории экспертную встречу по этим вопросам представителей стран партнеров. По статистике за последний год в Узбекистане было выявлено в социальных сетях более пятнадцати группировок экстремистского характера, по которым были приняты соответствующие законные меры. Подразделения нацио-

нальной безопасности и новые отделы МВД по борьбе с киберпреступностью ежедневно сканируют социальные сети для оценки дальнейших действий подразделений.

Список литературы

1. Минаев В. А., Купцов М. И., Вайнц Е. В., Киракосян А. Э. Моделирование противодействия терроризму и экстремизму в информационной сфере // Вестник Воронежского института ФСИН России. 2017. № 4. С 107–122.

2. Информационное противодействие терроризму и экстремизму : сборник статей Международной конференции АТЦ СНГ, 2015 176 с.

Бабакова А. В.[1]**,**
курсант 281 взвода факультета подготовки сотрудников полиции для подразделений по охране общественного порядка Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.,***
заместитель начальника кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ КОНТЕНТУ В СЕТИ ИНТЕРНЕТ

Влияние деструктивного контента на сознание окружающих – это новая проблема XXI в. Количество пользователей в сети неуклонно растет. Каждый может получить доступ к сети, и современные дети учатся печатать гораздо быстрее, чем писать в школе. Вместе с возможностями и благами интернета, они так же сталкиваются с его отрицательной чертой. Не каждый взрослый пользователь способен противостоять угрозам и негативному воздействию в интернетной среде, так несовершеннолетний пользователь в силу возраста может подвергнуться огромной угрозе и столкнуться с непоправимыми последствиями.

Что же такое деструктивный контент, и чем он опасен?

Для начала, стоит ознакомиться с таким понятием как «контент». Контент представляет собой полезную информацию, которая должна удовлетворить интерес аудитории сети интернет, и выражена в различных формах. Проще говоря, это все, что пользователь сети может прочитать, услышать или увидеть. Контент, в свою очередь, направлен на формирование у пользователей представления, мнения и впечатления на определенные вещи. Когда нужно сыграть на эмоциях людей, производят яркий цепляющий контент – например, вирусные промо-ролики, игровой интерактив. Если осуществляется продажа высокотехнологичного оборудования, используется сухой доходчивый язык общения с узкими отраслевыми профессионалами через цифры и аргументы.

Так же стоит сказать, что контент способен подстраиваться, чтобы удовлетворить требования своих пользователей. И как у медали у контента, тоже есть своя темная и деструктивная сторона. Контент сети Интернет, быстро распространяется, является доступным, зачастую не имеет цензуры. На сегодняшний день избыток контента негативно влияет на пользователей.

Возвращаясь к проблеме влияния деструктивного контента на несовершеннолетних пользователей, стоит выделить несколько направлений:

– нежелательный контент;

– киберпреступность;

– виртуальные хищники;

---

[1] © Бабакова А. В., 2021.

– кибербулинг.

Все это наносит вред на несформировавшееся сознание детей. Так же имеет место такому понятию, как «мода», т. е. совокупность привычек, ценностей и вкусов, принятых в определенной среде в определенное время. Но в данном случае, мода носит деструктивный характер.

Отсюда такое явление, как массовые самоповреждения и серия суицидов среди подростков. Их можно рассмотреть на примере одного из наиболее громких случаев.

23 ноября 2015 г. 17-летняя девушка Рената Камболина (более известная по нику Рина Паленкова) покончила собой на железнодорожных путях. Это событие стало отправной точкой для целой волны создания подростковых пабликов суицидальной тематики.

Фотографии судмедэксперта, которые были сделаны на месте происшествия, оказались в сети, после чего быстро распространились по молодежным пабликам и беседам. Возросший интерес к странички девушки в социальных сетях привлек сотни новых подписчиков. Ситуацию усугубила и активная виртуальная жизнь самой девушки – при жизни она вела популярный паблик «Психиатрическая больница», там девушка постила информацию депрессивной и суицидальной тематики.

Тренд 2021 года – размещение в TikTok видеороликов с падением с большой высоты, некоторые из которых закончились трагично.

Здесь следует не забывать, что подобному поведению способствуют и такие причины как:

– дисфункциональная семья – первичный институт социализации, обстановка в которой влияет на дальнейшую жизнь ребенка;

– проблемные отношения – не стоит обесценивать чувства ребенка, первый опыт, бывает крайне болезненным;

– проблемы в учебе;

– окружение.

Волна популярности «депрессивно-суицидальных» пабликов, отчасти возросшая после гибели Ренаты, стала подспорьем для появления «кураторов групп смерти». Это люди, которые начали создавать для проблемных подростков своеобразные игры с пугающими заданиями – деструктивное поведение (прогулки по крышам, употребление ПАВ, самоповреждение) и в конечном итоге – суицид.

Благодаря обилию тематических пабликов и групп кураторам не нужно прилагать усилия, чтобы найти себе клиентов. Они изучают странички потенциальных жертв, чтобы заслужить доверие и довольно скоро оказываются для сепарирующих от родителей подростков новым авторитетом, дают несовершеннолетнему иллюзию, так необходимого им, принятия.

Большинство заданий включает в себя фото- и видеоотчеты. Так куратор получает компромат и возможность для шантажа. Поэтому множество подростков с этого этапа «играют» до последнего – страшно быть опозоренным в ин-

тернете и стыдно обратиться к родителям за помощью (особенно, если в отношениях с ними есть проблемы).

Так же появляются в сети деструктивные флэш-мобы. Некоторые критики полагают, что флешмобы ведут к вседозволенности, провоцируют массовые хулиганства. Флешмобы также могут проводиться определенными людьми в корыстных целях: под видом флешмоба организовать преступление и т. п.

Некоторые участники акций могут заранее знать о преступном характере планируемого флешмоба. Такие флешмобы называют флеш-робингами.

Так в 2021 г. несовершеннолетних пользователей агитировали участвовать в несанкционированных митингах в пользу освобождения оппозиционера А. А. Новального.

Интернет-растлити. Эту проблему тоже можно осветить через призму одного из самых громких случаев. Преступник, который умело манипулировал подростками в интернете, находясь при этом в тюрьме. Мужчина находил в сети «проблемных» детей с нарушенным сознанием и обещал им мистические способности за выполнение заданий и «служение Сатане». Педофил принуждал подростков снимать на камеру компрометирующие видео – сначала обнаженные кадры, позже – самоистязания. Этот материал мужчина позже успешно продавал на специализированных сайтах «темного» интернета. А после выхода из тюрьмы злоумышленник пошел еще дальше – он начал встречаться с этими подростками в реальной жизни, поил алкоголем и растлевал.

Вербовка детей. Помимо озлобленных подростков и извращенцев в интернете подростков поджидают и просто ушлые люди с желанием быстрого заработка. Они так же втираются в доверие к ребенку, получают «компромат» − и требуют деньги или заставляют подростка заниматься преступной деятельностью (например, разносить и продавать наркотики). Известны и случаи вербовки молодежи террористическими группировками. Взрослые «брутальные» мужчины знакомятся с юными девушками, проявляют к ним заботу и внимание, предлагают переезд. Так, например, случилось с российской студенткой Варварой Карауловой, которую успели перехватить на границе Сирии.

На сегодняшний момент роль деструктивного контента продолжает расти. А попытки его контролировать и минимизировать, не достаточно эффективны. При удалении контента и блокировании страниц деструктивных пользователей, в сети позволяют лишь на время приостановить их влияние. Избавление от подобного контента сегодня не гарантирует того, что он не появится завтра, ведь спрос рождает предложение.

По моему мнению, следует уделять большее внимание информационному просвещению среди несовершеннолетних. Ребенку важно осознавать, что в мире есть люди, которые всегда его поддержат. Не всегда это обязан быть кто-то из родственников. Очень часто его роль играет значимый взрослый. Важно, чтобы он был доступен для ребенка. Этот человек позволит подростку не бояться, проявить себя и найти то, чем ему действительно нравится заниматься. К нему ребенок сможет прийти, чтобы получить ободрение и поддержку, что бы с ним ни случилось в жизни. Нужно не просто пытаться оградить ребенка от деструктивного контента, а заинтересовать его полезным контентом.

Список литературы:

1. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В.Гончар и др.]. М. : Московского университета МВД России имени В.Я. Кикотя, 2021.

Гера Ю. М.[1]*,*
курсант 282 взвода факультета подготовки сотрудников
для подразделений по охране общественного порядка
Московского университета МВД им. В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ

XXI в. считается временем, когда технический прогресс стал на шаг впереди человечества, а это значит, что информационные технологии и информационно телекоммуникационная сеть Интернет имеет большое значение в деятельности каждого человека в настоящее время.

Для того, чтобы иметь представление о состоянии преступности в сфере использования информационно телекоммуникационных технологий или в сфере компьютерной информации, необходимо обратиться на официальный сайт Министерства внутренних дел Российской Федерации. Анализ статистических сведений о состоянии преступности за январь–сентябрь 2021 года свидетельствует о том, что за январь–сентябрь 2021 года было совершено 402980 тысяч преступлений. Это говорит о том, что преступники уже довольно хорошо освоили данную сферу, для того чтобы бороться с ними у правоохранительных органов должны быть нужные знания и инструменты для пресечения данных преступлений. В своей работе я бы хотела рассказать о том, как открытые источники информации в информационно-телекоммуникационной среде при правильном использовании смогут помочь сотрудникам правоохранительных органов в борьбе с преступностью. В данной статье мы бы хотели рассказать, о том, как открытые интернет источники помогут правоохранительным органам в борьбе с преступностью.

Для начала необходимо разобраться, что представляет собой открытый источник информации и закреплено ли на законодательном уровне данное понятие. В федеральном законе от 27 июня 2006 г. № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации» я нашла схожее понятие с тем, что нас интересует. В ст. 7 ФЗ-№ 149 говорится об общедоступной информации, как о сведениях и информации, которая размещается ее обладателями в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

Для того, чтобы правильно воспользоваться информацией сначала необходимо точно сформировать запрос, далее определить источник информации, до-

[1] © Гера Ю. М., 2021.

быть информацию, а именно извлечь ее из источника, и наконец ознакомиться с информацией и оценить результаты поиска.

Информация из открытых источников имеют свои плюсы и минусы, необходимо понимать, что такая информация требует минимальных затрат для ее получения; меньше рисков ее использования; информация легко доступна; нет правовых проблем (приватность, авторские права). Минусами являются, то что в настоящее время объем информации, находящейся в интернете превышает способность человека ее обработать и проанализировать, это и является большим минусом в поиске нужных сведений, вторым минусом будет являться то, что на верификацию такой информации, то есть ее проверку и подтверждение достоверности может потребоваться большое количество времени, но данное действие необходимо, поскольку могут появиться правовые последствия.

В настоящее время в Российской Федерации происходит разработка сервиса для поиска информации о гражданах по открытым источникам. Данным направлением занимается холдинговая компания «Автоматика» совместно с «Национальной инжиниринговой корпорацией» (НИК) и ООО «Ти Хантер», это компании реализует разработку систем и комплексов, которые служат для обеспечения защиты информации. Холдинг «Автоматика» осуществляет проектирование, производство и модернизацию технических средств и систем защищенной связи, развивает технологии и методы криптографической защиты информации, системы автоматизированного управления и аппаратно-программных комплексов, разрабатывает IT-решения для заказчиков различных отраслей экономики.

Концепция данного сервиса будет заключаться в том, чтобы сознать такую платформу, которая будет заниматься поиском и предупреждением киберпреступлений. Данная технология будет анализировать информацию в открытых источниках и на ее основании предоставлять отчеты о личности подозреваемых. Решением будут пользоваться правоохранительные органы и крупные компании, а также и крупные компании, которые смогут помогать в расследовании киберпреступлений.

Данный сервис будет строиться на технологии Open Source Intelligence или разведки по открытым источникам, она основывается на поиске, выборе и сборе разведывательной информации из общедоступных источников, а также ее анализ. Один из разработчиков говорит о том, что программа должна работать следующим образом: следователь должен загрузить в систему e-mail или номер телефона подозреваемого, а программный комплекс сопоставит с этим массивы данных. В результате этого сотрудники ОВД получать информацию о личности подозреваемого.

Следует привести некоторые открытые источники информации, использование которых может способствовать раскрытию и расследованию киберпреступлений.

– tp.tja.pl – сайт с телефонным справочником, для поиска в справочнике необходимо выбрать регион и ввести, по крайней мере *фамилию имя или/и номер телефона*;

– intelx.io – его задача заключается в разработке и обслуживании поисковой системы и архива данных. Найдет адреса электронной почты, домены, URL-адреса, IP-адреса, CIDR, адреса биткойнов, хэши IPFS и т. д.;

– kribrum.io – «публичный поиск» является уникальным сервисом, с помощью которого возможно искать публикации русскоязычных пользователей в социальных сетях, на форумах, а также статьи на сайтах федеральных и региональных СМИ Российской Федерации и стран ближнего зарубежья. В настоящее время Поиск ведет мониторинг более 5 тыс. сайтов и социальных сервисов. В базе «Публичного поиска» содержится информация почти о 2 млрд публикаций за последние шесть месяцев от 130 млн пользователей интернета;

– otx.alienvault.com – делится последней информацией о возникающих угрозах, методах атак и злоумышленниках, способствуя повышению безопасности всего сообщества;

– ipinfo.io – С помощью IP-info можно точно определить местоположение ваших пользователей, настроить их взаимодействие, предотвратить мошенничество, обеспечить соответствие требованиям и многое другое.

Таким образом, можно сделать вывод о необходимости использования открытых источников информации в информационно-телекоммуникационной сети, поскольку это позволить сделать шаг вперед в борьбе с киберпреступностью. Так как данная сфера преступлений с каждым годом набирает обороты и постоянно совершенствуется, что нельзя сказать о механизмах и способах борьбы с данным видом преступлений, поэтому необходимо направлять средства для реализации и сознания технических программ, которые будут оказывать помощь правоохранительным органам.

Список литературы

1. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Горшкова М. С.[1]*,*
курсант 281 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

НЕКОТОРЫЕ ОПАСНОСТИ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

На пороге больших открытий, современного мышления и новых изобретений человечество все чаще сталкивается с киберпреступностью и ее любым проявлением в социуме. Возникает, по сути, новое цифровое мышление, некоторые люди превращаются в своеобразных роботов, которые в свою очередь, порой, не могут отличить реальность от вымышленного мира иллюзий цифрового пространства. Хорошо это или плохо, как и в любой существующей сфере имеются и плюсы, и минусы, на уровне прогресса, с параллельной стороны присутствует и регресс. Цифровая трансформация может внедряться только после изучения всех уязвимостей и обеспечения полной безопасности внедряемых продуктов. Как же это себя проявляет?

Современный бич прогресса – цифровая подпись. Это средство идентификации человека, использующего программный продукт. Хорошо, что общество не отстает от стран Запада и идет в ногу со временем, но есть и темные углы модернизированных возможностей. Ведь не стоит забывать и о мошенниках, разгуливающих на просторах всемирной паутины. Их возможности становятся шире, а навыки – хитрее. Каждый, преступник промышляющий в данной сфере имеет багаж знаний и достаточно подкован и в правоприменении своих возможностей.

Если мы обратимся к официальным данным МВД, то по статистике за последние два года все шире распространено мошенничество в отношении людей преклонного возраста и малолетних лиц. Их действия легко распознать, но порой их ухищренные методы могут повлиять на добрых старушек и наивных детей. Это происходит таким способом – как выяснило издание 47 News, оформить электронную цифровую подпись очень просто. Если известны СНИЛС и данные паспорта, то достаточно нескольких тысяч рублей и фотошопа. Журналист Юлия Гильмшина приобрела подпись за генерального директора издания. И в итоге, фирма, куда обратилась девушка пошла на встречу и выдала подпись за шефа, «который не хочет заниматься бюрократией». Так и выходит, что получена электронная подпись человека, который, по сути, сам никуда не обращался [5]. Это небезопасно.

Разберем биометрику (возможность распознавания людей, благодаря их физическим или поведенческим чертам) – используются в качестве формы управления и контроля доступа. Все бы ничего, и какая бы надежная не была защита, везде можно найти «лазейки» и обмануть систему. Так же и тут, многие умельцы своего дела искусно владеют «хакерскими» способностями.

Разберем один из самых распространенных способов получения биометрики злоумышленниками. Гражданину проходит звонок на телефон от незнакомого номера, конечно же человеческое любопытство берет верх, и после того, как он попался на уловку и поднял трубку, нашей жертве представляются сотрудником банка, или государственным служащим, после же предлагают ответить на несколько заезженных вопросов, на которые потребуется два ответа либо да, либо нет. Стоит отметить, что данные вопросы столь компрометирующие, что у гражданина сразу же рвется ответ наружу, и этот ответ положительный, что и нужно нашим злостным нарушителям закона. Киберпреступники в свою очередь, во время разговора с человеком, записывают его данные, если быть точным его голос. Далее, когда негодяи добились своего, разговор с оппонентом благополучно прекращается, а ребята в белых воротничках идут промышлять свои незаконные делишки.

Конечно же стоит упомянуть и о столь пугающем и масштабном проекте Билла Гейтса – чипирование населения. В наше время, благодаря короновирусу стало распространяться выражение антипрививочников, о том, что это таким способом человеком можно будет управлять. Считая это радикальным методом воздействия и сея зерно сомнения в сердцах доверчивых граждан. И правда, в России, и странах СНГ сейчас проводят опыты на животных и насекомых по внедрению микрочипа. Ученые утверждают, что это инновационная технология позволит современному человеку стать более технологичным и мобильным в сфере IT-технологий. По сути своей, данный микрочип имеет множественные функции, например, это может быть и ключ от машины, от дома, заработная карта, код доступа к банковским счетам и многое другое. Один маленький чип, размером с крохотное зернышко заменяет столько средств коммуникации и дает больший спектр возможностей. И да, это намного удобней, много места не займет и по пути на работу не потеряется.

Подведя итог вышесказанному, хотелось бы сделать вывод, несмотря на стремительное развитие цифровых технологий, не стоит забывать и о безопасности их внедрения. Я могу утверждать, что поспешное, необдуманное, неподготовленное и соответственно небезопасное внедрение технологий – недопустимо и приводит к росту соответствующих преступлений, так как этими уязвимостями и недоработками оперативно пользуются преступники. Мошенничество в техническом прогрессе активно развивается, не стоит забывать про креативность и находчивость злоумышленников, именно поэтому каждый должен совершенствовать свои познания в данном направлении и развивать свои навыки в современно-технических реалиях [6].

Список литературы

1. Осипенко А. Л. Сетевая компьютерная преступность. Омск, 2020. С. 109–110.
2. Oxford English Dictionary // URL: http://www.askoxford.com/ (дата обращения: 31.10.2021).
3. Cambridge Advanced Learner’s Dictionary // URL: http://dictionary.cambridge.org (дата обращения: 31.10.2021).
4. Кашлев Ю. Б. Становление глобального информационного общества и место России // Информация. Дипломатия. Психология. 2020. С. 18–20.
5. Теневая экономика и экономическая преступность // Информационные новости. 2021.
6. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов : XI Международная конференция. М., 2021. С. 187.

Ибришим А. П.[1]*,*
курсант 282 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ОСОБЕННОСТИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ ПРИ ПОМОЩИ БАНКОВСКИХ КАРТ

В современном мире нельзя представить жизнь человека без наличия банковского счета. Мы взаимодействуем с банковскими счетами: получаем заработанную плату, пенсии, оплачивает свои покупки, заказы в интернете, коммунальные услуги – это лишь малая часть того, с какими сферами связаны банковские счета. Бесспорно, высокий процесс в данной области значительно упрощает нашу жизнь. Мы можем не только проще и быстрее оплачивать услуги, но и вести учет потраченных нами финансов.

Однако, несмотря на все эти плюсы у «электронных денег» есть весьма значительный минус – плохая защищенность. Помимо того, что человек сам мог ошибиться при вводе реквизитов для оплаты услуг или же злоумышленник может завладеть данными карты с целью собственного финансового обогащения. У мошенников в арсенале имеется огромное количество способов завладения реквизитами карт с последующим хищники электронных денежных средств.

Перечислим некоторые из них:

1. Получение данных с использованием вредоносных программ, которые попадают на наши смартфоны и дублируют вводимую нами информацию на сервера злоумышленников, например, при авторизации в личном кабинете своего онлайн- банка;

2. Создание «зеркальных» сайтов, которые визуально похожи на оригинал, но на самом деле являются уловкой мошенников;

3. Продажа на всем известных сайтах объявлений, где злоумышленники в описании к товару оставляют ссылку на якобы оформление доставки, а на деле вводит данные для оплаты несуществующего товара;

4. В социальных сетях рассылают сообщения с просьбами перевести деньги на карту, переслать код подтверждения или пройти по ссылке, также существуют иные многочисленные способы, которые обозначим позднее.

В своих научных трудах Н. А. Лопашенко утверждает, что цифровое мошенничество утратило свою физическую форму и полностью перенеслось в виртуальное пространство, в сферу IT-технологий.

На этом фоне широкое распространение получили кражи с банковского счета. Относительно предшествующего года их массив увеличился до 96,9 тыс.

При этом отмечается замедление темпа прироста их числа до 6,2 %. Наиболее подвержены таким преступным посягательствам (в расчете на 100 тыс. населения) были жители Амурской области (139,9, Россия: 66), Республики Карелия (128,3) и Удмуртской Республики (116,9).

В январе – июле 2021 г. зарегистрировано около 194,8 тыс. различных мошенничеств.

Это на 6,3 тыс. больше, чем годом ранее. Их доля в структуре преступности на протяжении последних лет последовательно увеличивается и составляет 16,4 %. Наиболее распространены мошенничества в Ямало-Ненецком автономном округе (213,6 фактов на 100 тыс. жителей), Мурманской области (196,7) и г. Москве (189,8), наименее – в Чеченской Республике (27,5), республиках Ингушетия (34,1) и Дагестан (46).

В структуре подобного рода хищений значительна (более 70 %) доля мошенничеств, совершенных дистанционно, с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (137,9 тыс.). Темпы их прироста относительно начала года несколько замедлились и по итогам 7 месяцев 2021 г. не превысили 8,2 %.

Практически на две трети сократился массив мошенничеств с использованием электронных средств платежа (до 6,2 тыс.). Годом ранее статистика фиксировала практически двукратное их увеличение. Каждый пятый случай зарегистрирован в Омской области (–4,2 %, 1,3 тыс.).

В структуре преступности киберпреступления занимают более четверти (26,6 %, 315,7 тыс.). При этом следует отметить, что темпы их прироста с марта текущего года замедлились практически вдвое (март +33,7 %; июль +15,7 %). В 39,2 тыс. случаев жертвами таких преступлений стали пенсионеры, в 3,9 тыс. – несовершеннолетние, в 1,6 тыс. – инвалиды I и II группы.

На этом фоне все меньше фиксируется грабежей (–20,4 %, 18,9 тыс.) и разбоев (–19,5 %, 2,5 тыс.). Жители республик Тыва (58), Карелия (39,6) и Челябинской области (34) в текущем году были наиболее подвержены таким посягательствам на 100 тыс. населения). Большинство грабежей (14,8 тыс.) и разбоев (2,5 тыс.) совершены в общественных местах.

Также приведем материалы судебной практики.

Гражданин К. обвинялся в совершении преступления, которое имеет признаки состава, предусмотренного п «г», ч. 3 статьи 158 Уголовного кодекса Российской Федерации, а именно «кража, совершенная с банковского счета». Преступление было реализовано при следующих условиях и обстоятельствах: 13 ноября прошлого года гражданин К. примерно в 7 часов вечера получил от гражданина С. банковскую карту банка ПАО « Почта Банк», принадлежащую последнему. Гражданин С. Добровольно дал свою карту гражданину К. для осуществления покупки продуктов питания гражданином К., а также сообщил пин-код. Но гражданин К. воспользовался электронными деньгами по своему усмотрению, причинив гражданину С. материальный ущерб в размере 1650 рублей. Свою вину признал и был приговорен к наказанию в виде лишения свободы.

Данный пример указывает на то, что хищение электронных денежных средств происходит не только способами, перечисленными ранее, где упомянуты различные средства совершения противоправного деяния, такие как вредоносные программы, «зеркальные» сайты и иные современные технологии, а также с использованием доверительных отношений между преступником и потерпевшим. Как бы сказанное не было банальным, но данный способ завладения данными банковских карт и содержимым банковского счета имеет место быть.

Другим примером может являться приговор суда Пермского края в отношении гражданина С., который 20 октября прошлого года нашел паспорт, принадлежавший гражданину К, утерянный им в виду собственной невнимательности. В паспорте была найдена записка с номером и ПИН-кодом банковской карты. Далее гражданин С. последовал в подземный переход для приобретения новой сим-карты. После покупки для следующего этапа реализации преступного умысла пришел в ближайшее отделение банка, где предоставив паспорт гражданина К. и представившись его именем попросил оператора привязать к банковской карте новый номер мобильного телефона, так как старый телефон вместе с симкартой были утеряны. Оператор, не подозревая незаконность услуги, выполнила необходимые действия для привязки нового номера телефона к банковской карте гражданина К. После чего, уже находясь дома, гражданин С. установил мобильное приложение онлайн-банка, ввел необходимые реквизиты найденной банковской карты и перевел все денежные средства на номер своего счета. Данными финансами распорядился по своему усмотрению.

Приговором суда был осужден к лишению свободы условно.

В данном случае завладение электронными деньгами были реализованы путем обмана сотрудника банка, введения его в заблуждение насчет принадлежности банковской карты гражданину К. и собственно невнимательности сотрудника банка при установлении личности собственника предоставленного паспорта.

Подведя итог вышесказанному, необходимо отметить, что способы хищения денежных средств с банковских счетов многочисленны и отличаются разнообразием. От банального сообщения ПИН-кода «другу» до использования различных современных компьютерных программ и информационно-телекоммуникационных сетей. Представителям правоохранительных органов необходимо учитывать постоянно меняющиеся методы совершения хищений, в виду совершенствования компьютерных технологий и технического развития населения, информировать граждан о фактах данного рода преступных деяний, особое внимание уделять более уязвимым и менее защищенным слоям общества, такие как пенсионеры и малолетние, ведь именно они в большей находятся в зоне риска при совершении преступлений в данной области.

Список литературы

1. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_5842/ (дата обращения: 20.11.2021).

2. Портал правовой статистики // URL: http://crimestat.ru/offenses_chart (дата обращения: 11.11.2021).

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_110699/ (дата обращения: 20.11.2021).

4. Судебные и правовые акты Российской Федерации // URL: https://sudact.ru/ (дата обращения: 20.11.2021).

Кузьмин И. А.[1]*,*
курсант 283 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

АКТУАЛЬНОСТЬ УСОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ РОССИИ

Миллионы данных в день попадает в киберпространство от его пользователей. В качестве примера можно взять портал «Государственных услуг» в каждом отдельном аккаунте содержится вся полная информация о пользователе от серии и номера его паспорта до его адреса регистрации и фактического места жительства. Мошенники, которым удается взломать такие базы данных получают карт-бланш и могут пользоваться данными пользователей как посчитают нужным, могут продать их через даркнет[2] или могут оставить себе для личного пользования.

Даже имея отличную защиту не всегда можно надеяться на ее надежность, прямым примером этого служит взлом персональной информации юзеров[3] Facebook 4 октября 2021 года. На популярной хакерской торговой площадке в даркнете были выложены для продажи данные более полутора миллиардов пользователей. Специалисты оценили данный факт, как «самое большое количество утекших данных Facebook». В первую очередь, это огромный удар по кибербезопасности и это дает нам понять, что хакеры способны обойти любую современную защиту. И просто взять, и выложить такое огромное количество аккаунтов в даркнете то есть, человек купивший эти данные, сможет узнать о юзерах абсолютно любую информацию, это просто огромный провал, что самое интересное в даркнете невозможно вычислить изначальную точку, изначальный IP-адрес[4] того пользователя который выставил на продажу аккаунты Facebook.

---

[1] © Кузьмин И. А., 2021.

[2] DarkNet («Скрытая сеть», «Темная сеть» или «Теневая сеть») – сегмент интернета, который скрыт из общего доступа.

[3] Это слово выступает заимствованным термином из английского языка. Оно происходит от глагола «use», что переводится как «использовать».

[4] IP-адрес (сокращение от англ. Internet Protocol Address) – уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к локальной сети или интернету.

В исследовании стан мира по уровню подверженности киберугрозам за 2020 г. интернет ресурса «10 GUARDS» указаны данные о том, какие страны наиболее уязвимы, а также наименее уязвимы и те страны, у которых среднее промежуточное значение. Индекс подверженности киберугрозам (CEI – Cybersecurity Exposure Index) по странам представлен от 0 до 1. Он показывает: чем выше оценка, тем больше та или иная страна уязвима перед лицом кибератаки, тем самым соответственно ниже и ее уровень кибербезопасности.

Индекс подверженности киберугрозам (CEI) по странам представлен от 0 до 1. Он показывает: чем выше оценка, тем больше страна уязвима перед лицом кибератак и, соответственно, тем ниже ее уровень киберзащищенности.

Уровень подверженности киберугрозам	Значение
Очень высокий	0.800 – 1.000
Высокий	0.600 – 0.799
Средний	0.400 – 0.599
Низкий	0.200 – 0.399
Очень низкий	0.00 – 1.199

По данным этого исследования из 108 стран наименее подвержена киберугрозам Финляндия, за ней следуют Дания, Люксембург, Австралия и Эстония.

Российская Федерация по данным этого исследования находится на 44 месте из 108 и имеет индекс подверженности киберугрозам 0.528, что является средним уровнем подверженности киберугрозам. На мой взгляд, это неплохой результат, но следует стремиться к лучшему и повышать уровень киберзащищенности.

По данным «Интерактивной карты Киберугроз» которая основа на данных «Лаборатории Касперского» на территории Российской Федерации за временной период с 7 по 14 ноября 2021 г. было выявлено 7801125 Киберугроз. Это довольно большая цифра, она позволяет задуматься о том, что в современном устройстве мира, государство должно и обязано обеспечивать свою Кибербезопасность, развивать технологии в этой сфере и не то, чтобы «быть вровень с киберпреступностью по уровню развития технологий, а предугадывать и быть на шаг впереди»

Таким образом, подводя итоги моих высказываний, нужно отметить, что технологии, используемые в Российской Федерации по выявлению и устранению Киберугроз, находятся на среднем уровне по сравнению с некоторыми другими странами мира. Это не плохой результат, но, по моему мнению, это актуальная проблема и следует не останавливаться на достигнутом результате, а продолжать улучшать и усовершенствовать защитные программы, для дальнейшей более качественной защите данных не только государственных органов Российской Федерации, но и самих пользователей.

Список литературы

1. Русско-Американский словарь терминов и определений в сфере информационной безопасности.

2. Шапошников А. А. Криминологическая характеристика личности киберпреступника // URL: https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-lichnosti-kiberprestupnika-1.

3. «10 GUARDS» // URL: https://10guards.com/en/#blog.

4. Интерактивная карта киберугроз // URL: https://cybermap.kaspersky.com/ru/stats#country=213&type=OAS&period=w.

5. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Кушнин А. К.[1]*,*
курсант 282 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ДАРКНЕТ – ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ

На современном этапе развития технологий и робототехники, не стоит забывать и об истоках создания интернета. За последние два десятилетия гаджеты стали неотъемлемой частью жизни человека. Мы не можем представить свою жизнь без связи, стоит только появиться значку «нет сети», сразу же у среднестатистического пользователя появляется паника в глазах и насущный вопрос, а что же делать?

Признать честно, XXI в. поистине век информационных технологий и открытий. Цифровизация пришла к нам на помощь во многих делах, и трансформировала нашу деятельность в электронную работоспособность. С приходом новых технологий появляются и иные проблемы, например, взлом и похищение личных данных, вопросы юрисдикции, идентификация пользователя и многое другое. Именно поэтому стоит обратить внимание на теневую сторону всеми известной системы объединенных компьютерных сетей для хранения и передачи информации, которая в свою очередь ускользает из сферы правового регулирования.

Данное понятие пришло к нам в 70-х гг. прошлого столетия, тогда активно развивался и процветал нелегальный бизнес (стоит упомянуть, что и по сей день в «закрытой сети» продолжает данный бизнес продолжает набирать обороты).

Разберем подробно, что же на самом деле представляет из себя скрытая сторона интернета для обычных пользователей. Анонимностью сейчас никого не удивишь, на пороге век информационных открытий и новшеств. За обычным рядовым пользователем сетей следят системы, от которых не скрыться. Что же делать? На помощь приходит даркнет, на который легко попасть без усилий, достаточно проникнуть в его структуру и скрыться от различных служб. Попасть на платформу даркнета можно благодаря Tor Browser или I2P.

Tor распределяет ваш трафик по сети, которая состоит из нод (или ретрансляторов) – тысяч серверов, которые создаются и поддерживаются доброволь-

---

[1]

цами, чтобы обеспечить безопасность и анонимность. Каждый раз, когда вы подключаетесь к Tor, он строит самый быстрый и безопасный маршрут.

I2P – это прокси-сервис, который пропускает через себя весь трафик, включая мессенджеры и другие приложения. Он намного медленнее, чем Tor, но обеспечивает и анонимность, и конфиденциальность.

В законодательстве Российской Федерации отсутствует определение даркнета. Тем не менее, можно выделить ряд значимых для правового регулирования признаков:

– даркнет – это информационно-коммуникационная система для взаимодействия пользователей (так же как и открытый интернет);

– с точки зрения программного обеспечения основан на технологии TOR или его аналогах;

– обеспечивает анонимность и конфиденциальность своих пользователей;

– благодаря даркнету процветает преступная деятельность, которую сложно определить из-за зашифрованных IP-адресов.

Такая конфиденциальность личности пользователя может ему сыграть на руку (например, для развития и продуктивности разговора), так и использоваться злоумышленниками, например, для продажи психотропных и наркотических веществ, а также и прекурсоров, по некоторым данным МВД, на площадке продаются видеоролики для любителей порнографии с детьми, так и продажа самих людей и органов (черный рынок), продажа оружия, заказные убийства и т. п.

Так же затронем тему оплаты всех вышеперечисленных услуг – биткоин. Все варьируется в различных ценниках на сложность разных услуг. Благодаря именно криптовалюте правоохранителям сложно найти какую-либо информацию и выследить злоумышленников, так как базы не имеют абсолютно никакой информации о транзакциях и счетах.

Подведя итог, хотелось бы сказать, что в первую очередь нужно активно развиваться в сфере технологий не только различным службам, но и самим гражданам, дабы обеспечить себе спокойствие и быть уверенным, что твои данные не будут похищены и не использованы на черном рынке. Бизнесу целесообразно внедрять только безопасные технологии, проверенные и апробированные в пилотных регионах. Даркнет представляет собой инструмент, который приобретает общественную опасность благодаря злым умыслам своих пользователей. Необходимо выработать правовые и технические средства борьбы с опасными проявлениями в сети. Востребованы новые подходы, новые кадры со свежим взглядом на мир, и новые идеи решения глобальной проблемы.

Список литературы

1. Мэтт Иган. На темной стороне интернета: Что такое Dark Web и Deep Web? // URL: https://www.dgl.ru/articles/na-temnoy-storone-interne.

2. Голик Д. И., Ганжа Е. А., Коломоец А. В. Темная сторона интернета. Ее суть и принцип работы // URL: https://elibrary.ru/item.asp?id=31877134.

3. Мерзликин П. А. Что продают в русскоязычном Dark Web? // URL: https://paperpaper.ru/dark/.

4. Garman C., Green M., Miers I. Accountable privacy for decentralized anonymous payments // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017. С. 81–98.

5. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Маслов А. П.[1]*,*
командир отделения 283 взвода факультета
подготовки сотрудников полиции для подразделений
по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ВЛИЯНИЕ КОМПЬЮТЕРНЫХ ИГР НА ДЕВИАНТНОЕ ПОВЕДЕНИЕ ПОДРОСТКОВ

Девиантное поведение представляет собой отклонение от привычных (принятых в обществе) норм поведения. В современном мире весомую роль в жизни почти каждого подростка составляют компьютерные игры. Компьютерным играм уделено сейчас весомое количество времени и места в жизни подростка, что безусловно влияет на процесс развития и формирования будущего и подрастающего поколений. Этот феномен требует углубленного изучения для понимания и прогнозирования возможных последствий влияния компьютерных игр на социальное развитие и формы мышления у подростка, пока недостаточно разработан в трудах современных научных деятелей.

Начиная с кликеров на телефоне и заканчивая многочасовыми играми за персональными компьютерами. В связи с этим на нынешнем этапе развития общества социальные и экономические проблемы, психологическое расстройства и стрессы все чаще и чаще приводят к перенапряжению человека. Недовольство реальной жизнью, отвращение к ней, ее несправедливости, злу и желание отдохнуть от его осложнений становятся одной из необходимостей в жизни современного человека, причем форм и способов отхождения от реальности, которые может выбрать подросток, крайне много и не всегда общественно одобряемы, а иногда даже и порицаются обществом. Как раз одним из таковых способов является девиантное поведение, когда вся жизнь подростка, его мироощущение, интересы и привычки начинают зависеть от различных факторов (компьютерных игр, наркотиков, алкоголя, правонарушения, преступления и т. п.). Подростки страдают в ожидании выхода новых компьютерных игр, а когда появляются анонсы об их выпуске, совсем теряют над собой контроль.

Согласно позиции Т. А. Донских и Ц. П. Короленко «имеется ряд существенных признаков, характерных для зависимости от игр как одного из видов девиантного поведения: Постоянная вовлеченность, увеличение времени, проводимого в ситуации игры. Изменение круга интересов, вытеснение прежних мотиваций игровой мотивацией, постоянные мысли об игре. «Потеря контроля», выражающаяся в неспособности прекратить игру как после большого

выигрыша, так и после постоянных проигрышей. Состояния психологического дискомфорта, раздражения, беспокойства, развивающиеся через сравнительно короткие промежутки времени после очередного участия в игре, с труднопреодолимым желанием снова приступить к игре. Быстро нарастающее снижение способности сопротивляться соблазну.»

Сейчас проблема ухудшается тем, что современные компьютерные игры специально устроены так, что в течении всей игры у подростков возникает отчуждение, облегчение от любого напряжения, отвлечение от внешних проблем, а значит, игра считается как приятное провождение времени, допустимая в социуме форма досуга, при этом у подростка постепенно развивается зависимость. В связи с этим многие исследователи (И. Бурлаков, М. Иванов, Ю. Ковш, Г. Кочетков, Е. Лысенко, Г. Мешков, В. Чаговец, Б. Шлимович, А. Шмелев и другие ученые считают компьютерные игры огромной социальной проблемой. Они считают, что в настоящий момент програмируются и предлагаются разновидности игр, которые стали очень простыми в подходе и доступными для детей и подростков. Аддикция к игре появляется тогда, когда после игры в нее подросток начинает постоянно думать об игре и пытается вновь вернуться в нее. Подросток начинает рассказывать об этом, зовет друзей поиграть в эту игру. Постепенно этот способ проведения времени все чаще и чаще повторяется, становясь главным способом времяпрепровождения, тем самым деструктивно воздействуя на подростка.

Компьютерные игры так же представляют собой опасность, связанную с ухудшением физического и психического здоровья, трата в пустую большого количества материальных средств, потеря большого количества времени. Причинами ухода из реальной жизни в виртуальную становятся: нехватка общения с родителями, родственниками, друзьями, неблагоприятный климат в обществе, плохая обстановка в кругу друзей и близких, оскорбления и нападки со стороны сверстников, отсутствие контроля извне.

В трагедиях с участием подростков не редко винят компьютерные игры. Одни специалисты считают, что различные жанры игр, например, как шутинги и файтинги и провоцируют насилие. В других исследованиях говорится, что игры снижают стресс и помогают социализироваться. Выводы о влиянии компьютерных игр делали различные научные деятели: компьютерные игры со сценами насильственных действий провоцируют агрессивное поведение.

Игры усиливают агрессию у агрессивно настроенных людей. Подростки, которые плохо успевают в учебе, обожают проводить время за компьютерными играми. Жестокие игры оказывают на детей больше влияния, чем проблемы в семье и со сверстниками. Краткосрочный эффект от игр гораздо меньше, чем считалось изначально. Детей чаще делают агрессивными не игры, а насилие в семье и буллинг в школе. Только 0,4 % разных форм агрессии могут быть вызваны жестокими видеоиграми. Релизы популярных игр отвлекают геймеров от правонарушений. Видеоигры со сценами насилия повышают стрессоустойчивость. Игры помогают подросткам поддерживать отношения со сверстниками.

Российские депутаты несколько раз выносили предложения о борьбе с видеоиграми путем совершенствования законодательства. Предпосылками для

этих предложений явились убийства, которые были совершены и организовывали подростки в различных учебных заведениях.

Например, в Москве в 2014 году, в Керчи в 2018 г. и в Казани в 2021 г. Ответ на этот вопрос неоднозначен. Так, ограничительные инициативы озвучивали и политики Соединенных штатов Америки. В 1993 г. ряд сенаторов устроили серию слушаний в Конгрессе из-за игр «Mortal Kombat» и «Night Trap», усмотрев в них излишнюю жестокость. После продолжительных прений сторон производителям компьютерных игр пришлось создать рейтинговую систему с возрастной маркировкой для игр. Также компании стали предупреждать покупателей о сценах насилия и другого аморального контента в играх. С 1994 г. за маркировку в играх отвечает негосударственная некоммерческая организация «Entertainment Software Rating Board» (далее – ESRB). Перед изданием игры и выпуском ее для всей аудитории и на рынок создатели обязаны отправить в ESRB сценарий игры и описать эпизоды, в которых встречается насилие, секс, мат, употребление алкоголя и так далее. По итогам ESRB ставит на данную продукцию возрастной рейтинг. Еще одной игрой, которая вызвала большую волну недовольств конгресменов, стала Doom. В 1999 году произошло массовое убийство в школе «Колумбайн» в штате Колорадо.

Два ученика старших классов (Эрик Харрис и Дилан Клиболд) с помощью оружия и самодельных взрывных устройств и взрывчатых веществ убили дюжину человек и ранили в различной степени еще не менее 20 человек. Оба подростка увлекались компьютерной игрой «Doom» и создавали для нее различные самодельные уровни. Проверить связь между трагедиями с участием и подростков и наличием сцен насилия пытались в разные промежутки времени руководители страны такие как: Билл Клинтон, Барак Обама и Дональд Трамп.

В заключении следует отметить, что вывод играть в компьютерные игры или нет необходимо принимать в каждом конкретном случае индивидуально, исходя из психологических особенностей конкретного ребенка и особенностей игры. Наиболее жесткие игры, провоцирующие насилие и жестокость не должны находить свободного распространения.

Список литературы

1. Бурлаков И. В. Психология компьютерных игр // URL: https://cyberpsy.ru/articles/psychology_computer_games/.

2. Шалимович Б. Влияние компьютерных игр на подростков // URL: https://infourok.ru/nauchnoissledovatelskaya-rabota-vliyanie-kompyuternih-igr-na-podrostkov-451760.html.

3. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Солодов Е. А.[1]***,***
курсант 281 учебного взвода
факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.,***
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРОФИЛАКТИКА ДИСТАНЦИОННЫХ ХИЩЕНИЙ

На сегодняшний день невозможно представить свою жизнь без телефона и компьютера. Телефон стал нашим «продолжением руки», в котором мы храним практически все свои данные, начиная от банальных фотографий, заканчивая целыми сбережениями в банках.

Технологии намного упростили нашу жизнь. Можно заплатить за кредит одним нажатием, заказать продукты за 5 минут и не стоять в очереди, можно хранить весь фотоальбом в электронном формате и всегда получить доступ к фотографиям и так далее. Другими совами – информационные технологии экономят большое количество нашего времени. К сожалению, существует и обратная сторона такой медали. Мошенники научились без каких-либо проблем красть данные чужих людей различными способами. За последние пять лет число киберпреступлений выросло в 11 раз и составляет 510,4 тыс. случаев. Генпрокуратура утверждает, на кибермошенничества пришлось около 70 % всех хищений. Так же, почти в два раза увеличилось количество краж с банковских счетов и электронных кошельках, что на 2020 г. составляло 169,5 тыс.[2]

Наиболее распространенными дистанционными хищениями являются:

– получение реквизитов банковской карты при осуществлении купле-продаже товаров и услуг в интернет сайтах.

– взлом социальной сети и просьба в предоставлении денежных средств родственника или друзей.

– мошенничество через оформление кредита.

Человек оформляет кредитную заявку на непроверенном сайте, заполняет полностью свое ФИО, номер телефона и иные личные данные. Дальше, на номер этого человека поступает звонок от этого «банка» в котором работник утверждает, что заявка одобрена, но необходимо перевести определенное количество денег на уплату расходов, связанных с оформлением кредита. После того, как человек отправил определенную сумму денег, связь с банком прекращается.

Чтобы таких ситуаций не случалось, граждане должны обладать хотя бы самыми минимальными знаниями в области финансовой грамотности и проявлять осмотрительность и аккуратность при обращении с деньгами.

---

[1] © Солодов Е. А., 2021.

[2] Статистика МВД России.

Необходимо сказать, что зачастую мошенники входят в доверие к гражданам и представляются от лица сотрудников банка и сообщают, что карта была взломана и так далее. Смысл таких действий направлен на то, чтобы человек сказал полностью все данные карты, чтобы в дальнейшем можно было списать все сбережения оттуда.

Бывают случаи, когда мошенники получают удаленный доступ к телефону или компьютеру путем установки приложений для удаленного доступа, типа TeamViewer Это происходит путем использования методов социальной инженерии или через вирус на сайте и в дальнейшем, имея полный удаленный доступ к телефону, можно делать все что хочешь – перевести деньги на другой счет, получить все фотографии и иную личную информацию, даже взять удаленный кредит на максимально возможную сумму и перевести ее себе. К сожалению, такие преступления трудно доказываются и вероятность того, что преступника освободят от ответственности не маленькая. Фиксируется значительное количества условных приговоров за подобные преступления.

И так, для того, чтобы не стать жертвой мошенников необходимо придерживаться следующих правил:

1. При осуществлении интернет-диалога с неизвестным человеком, необходимо удостовериться в информации, полученной в ходе общения. Такой человек может представиться кем угодно – сотрудником банка, сотрудником правоохранительных органов, оператором сотовой связи и так далее. Если речь идет о ваших родных, к примеру: «Ваш муж попал в ДТП, необходимо срочно перевести деньги», необходимо вначале связаться с самим мужем для уточнения информации.

2. Никогда не сообщайте свои реквизиты от банковской карты и иную другую информацию, например, секретные коды и ответы на секретные пароли. Запомните, сотрудники банка никогда не попросят вас сказать реквизиты от карты.

3. Никогда не перечисляйте денежные средства на счета и номера телефонов, которые указал незнакомец.

4. При осуществлении каких-либо действии на интернет сайтах, проверяйте вначале сам сайт, так как он может оказаться фишинговый, потом проверяйте подлинность информации на этом сайте.

5. При утере банковской карты своевременно сообщайте об этом в банк, а также при смене номера телефона.

6. Не поддавайтесь на различного рода уговоров от незнакомцев, например, снятие сглаза, наведение порчи и т. д.

7. Финансово-кредитным учреждениям необходимо запретить порочную практику навязывания ненужных и опасных финансовых продуктов, например услуги дистанционное получение кредита. В сегодняшних реалиях потерпевшим от таких хищений необходимо признавать саму финансово-кредитную организацию, неспособную обеспечить безопасность внедренных продуктов.

Если так получилось, что с вашей банковской карты похитили денежные средства, необходимо в тот же день обратиться в банк, приостановить обслу-

живание счетов, на которые были отправлены деньги. После получения банковского ответа, обратиться в полицию.

В таких ситуациях огромную роль играет Участковый уполномоченный полиции. Он должен осуществлять постоянную профилактическую и разъяснительную работу с гражданами и индивидуальную работу с лицами, находящимися в группе риска. К такой группе относятся в первую очередь малолетние лица и пенсионеры. Только так мы сможем остановить лавинообразный рост интернет мошенничеств, угрожающий социальной стабильности нашей Родины.

Список литературы

1. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

2. Профилактика дистанционных хищений // URL: https://finance.rambler.ru/other/44088686-profilaktika-distantsionnyh-hischeniy/.

3. Статистика РБК // URL: https://www.rbc.ru/society/31 /08/2020 /5f48ea169a-79477e21e25d9d.

4. Статистика МВД России // URL: https://мвд.рф /dejatelnost/statistics.

Сухинина Я. В.[1]*,*
курсант 282 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Гончар В. В.****,*
заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРОФИЛАКТИЧЕСКИЕ МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРБУЛЛИНГУ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ

На сегодняшний день, повышенным значением обладает защита прав и законных интересов несовершеннолетних. В данном направлении реализуются различные меры, средства и методы со стороны государства, законных представителей несовершеннолетних и иных субъектов, задействованных в работе с несовершеннолетними.

В текущее время отмечаются тенденции к информатизации общества, что выражается и в активном использовании сети Интернет. Несомненно, в подобные процессы оказываются активно вовлеченными и несовершеннолетние граждане. Возможность применения информационных технологий несет в себе как положительные качества, так и в отдельных случаях негативную направленность. В рамках данной статьи будет рассмотрен профилактика кибербуллинг в отношении несовершеннолетних.

Общеизвестным является тот факт, что в понятие здоровья входят различные компоненты. Так, согласно п. 1 ч. 1 ст. 2 ФЗ «Об основах охраны здоровья граждан в Российской Федерации»: «здоровье – состояние физического, психического и социального благополучия человека, при котором отсутствуют заболевания, а также расстройства функций органов и систем организма» [2].

В таком контексте, следует говорить о необходимости сохранения психического и социального благополучия несовершеннолетнего, наряду с иными компонентами здоровья. Указанное направление весьма значимо и позволяет обеспечивать полноценное развитие несовершеннолетнего.

Появление кибербуллинга произошло сравнительно недавно и приравнивается к развитию сети Интернет и увеличению количества граждан, пользующихся всемирной сетью.

Интересную позицию высказывают К. Д. Хломов, Д. Г. Давыдов, А. А. Бочавер: «Агрессивное поведение в интернет-пространстве становится все более распространенным среди подростков в России и за рубежом. Кибербуллинг – один из наиболее новых и опасных с точки зрения последствий риск, с которыми сталкиваются современные подростки» [5, с. 276].

Действительно, в процессе кибербуллинга (может быть, как прямым, так и косвенным), происходит «травля» в интернете. Характерной чертой кибербул-

---

[1] © Сухинина Я. В. 2021.

линга является свободное размещение угрожающих материалов, унижающих честь и достоинство несовершеннолетнего, а также подверженность нападкам в любое время суток, вне зависимости от территориального расположения. Кроме того, последствия кибербуллинга могут привести к губительным, порой трагическим последствиям ввиду вовлечения в данный процесс большого количества случайных свидетелей.

В сравнении с нападками, например, в школе (во дворе и пр.), масштаб кибербуллинга является гораздо более обширным. Указанные факторы во взаимосвязи с особенностями развития психики несовершеннолетнего, приводят к глубоким переживаниям, депрессивным состояниям и иным негативным проявлениям в психологическом состоянии несовершеннолетнего, в том числе увеличивая уровень раздражительности, расстройства, болезненного восприятия окружающей действительности и др. Нарушения происходят как в эмоциональной сфере несовершеннолетнего, так и в его социальных связях.

Очевидная, высокая негативная направленность кибербуллинга требует поиска эффективных мер борьбы с ними и оказания помощи различного характера несовершеннолетним. С этой целью требуется формирование эффективных подходов к правовому регулированию мер охраны и защиты несовершеннолетних от кибербуллинга.

Представляется, что в указанном направлении используются как меры административного, так и меры уголовно-правового регулирования. Соответственно, следует говорить о профилактике, предупреждении и пресечении правонарушений и преступлений, прямо или косвенно связанных с кибербуллингом в отношении несовершеннолетних.

Если говорить о мерах административного воздействия, необходимо отметить органы, наделенные соответствующими административно-юрисдикционными полномочиями по отношению к работе с лицами. не достигшими совершеннолетия.

В частности, первостепенное значение приобретает деятельность комиссий по делам несовершеннолетних и защите их прав (далее – КДН и ЗП), общеобразовательных организаций, учреждений дополнительного образования, ПД в составе органов полиции, органов опеки и попечительства, а также уголовно-исполнительной системы и пр.

Очевидно, что КДН и ЗП осуществляют профилактические мероприятия, которые обладают в том числе, координирующим характером, позволяя объединить деятельность различных субъектов, задействованных в вопросах реализации профилактических мероприятий с несовершеннолетними на основании гл. 2 ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» [1].

Необходимо подчеркнуть, что КДН и ЗП, помимо назначения административного наказания, как орган профилактической направленности, устанавливает не только событие административного правонарушения, но и те условия, которые способствовали его совершению, в связи с чем, имеет полное право внести в соответствующие органы и организации, должностным лицам представление о принятии обязательных мер, направленных на устранение злонамерен-

ных, пагубных причин и условий. В свою очередь, те субъекты, которые такое представление получили, должны выполнить указанные требования и сообщить о тех мерах, которые были направлены на устранение таких причин и условий.

Итак, в системе субъектов, осуществляющих профилактические мероприятия (деятельность) с лицами, не достигшими совершеннолетнего возраста, центральное место отведено комиссии по делам несовершеннолетних и защите их прав, имеющие достаточно обширные полномочия в указанной сфере. В осуществлении профилактических мероприятий большое значение имеет взаимодействие КДН и ЗП с образовательными организациями, семьей и пр. Представляется, что существенным недостатком выступает отсутствие методических основ по борьбе с кибербуллингом в отношении несовершеннолетних. Наличие подобного документа смогло бы помочь работе КДН и ЗП, а также органов и организаций, входящих в систему профилактики по отношению к несовершеннолетним.

В специальной литературе неоднократно отмечалась важность уголовного противодействия. Так, по мнению К. А. Красновой, Д. И. Ережипалиева: «сочетание технологических и социальных факторов поощряет людей к участию в преступлениях или противоправных деяниях, таких как подстрекательство к самоубийству несовершеннолетних, а доступность Интернета для большинства российских семей расширяет аудиторию незащищенных от кибербуллицида детей. Существование и активная антиобщественная деятельность так называемых «групп смерти» позволяет говорить о них как о новом виде организованной преступности» [3, с. 82].

Как считает В. А. Мальцева, необходимо закрепить в действующем законодательстве Российской Федерации конкретные меры уголовно-правовой охраны несовершеннолетних жертв кибербуллинга [4].

Обобщая результаты настоящего исследования, стоит отметить, что на сегодняшний день, назрела необходимость в усилении административно-правовых и уголовно-правовых основ борьбы с кибербуллингом в отношении несовершеннолетних. По последнему основанию, необходимо говорить об усилении мер уголовной ответственности в связи с кибербуллингом, который приводит далее к тяжким, не редко, необратимым последствиям.

В частности, необходима разработка Методических основ работы правоохранительных органов по борьбе с кибербуллингом в отношении несовершеннолетних для применения в процессе профилактических и предупредительных мероприятий, привлекать к этой деятельности органы государственной власти субъектов и органы местного самоуправления.

Список литературы

1. Федеральный закон от 24 июня 1999 г. № 120-ФЗ (ред. от 24.04.2020) «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // Собрание законодательства Российской Федерации. 1999. № 26. Ст. 3177.

2. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ (ред. от 02.07.2021) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724.

3. Краснова К. А., Ережипалиев Д. И. Противодействие кибербуллициду как средство предупреждения суицидов несовершеннолетних // Юристъ-Правоведъ. 2017. № 3 (82). С. 78–84.

4. Мальцева В. А. Защита детей от кибербуллинга. Вопросы уголовно-правового регулирования // Закон и право. 2019. № 10. С. 95–99.

5. Хломов К. Д., Давыдов Д. Г., Бочавер А. А. Кибербуллинг в опыте российских подростков // Психология и право. 2019. Т. 9. № 2. С. 276–295.

6. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Милетенко Н. И.[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Путилов А. О.,***
врио заместителя начальника кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ НЕЙРОННЫХ СЕТЕЙ ПРИ РАЗРАБОТКЕ СОВРЕМЕННЫХ АНТИВИРУСНЫХ СРЕДСТВ

Компьютерный вирус – это вредоносная программа. Обычно вирус находится в одном или нескольких файлах операционной системы компьютера. Как правило, когда заражается чистый файл, он модифицируется таким образом, чтобы код вирусной программы вставлялся в исходный файл (так называемая хост-программа), и его запуск в какой-то момент времени инициировал запуск вируса. Однако некоторые вирусы запускаются полностью без вмешательства пользователя. Процесс запуска вируса включает в себя сканирование компьютера или сети для выявления новых жертв и их заражения. Некоторые типы вирусов не заражают файлы вообще, полностью находясь в памяти. Хотя различий между вирусами предостаточно, все они имеют одну важную характеристику, а именно способность к самовоспроизведению. Таким образом, компьютерный вирус может быть определен как программа, которая заражает другие программы и самовоспроизводится. Например, на основе методов искусственного интеллекта, в частности, нейронной сети.

Самые популярные методы обнаружения вирусов – обнаружение вирусов на основе сигнатур (характерных признаков), обнаружение на основе аномалий, эмуляция кода.

Выявить вредоносное программное обеспечение можно несколькими способами:

– сравнение программного обеспечения с известными файлами определений вирусов для поиска подходящих паттернов. этот подход использует существующие файлы вирусов для поиска шаблонов, по которым создаются файлы определений вирусов. новые файлы сравниваются с файлами определений вирусов для того, чтобы определить, являются ли они вредоносными;

– мониторинг поведения исполняемых файлов в системе, позволяющий обнаружить какие-либо аномальные действия, выполняемые ими (пример: запись в системные файлы). исполняемые файлы могут выполнять вредоносные действия только в том случае, если они выполняются пользователем. обычно эти файлы пытаются получить доступ к неавторизованным областям памяти на

компьютере или пытаются записать что-то в системные файлы. следовательно, можно искать эти действия и предупреждать пользователя о наличии вируса;

– запуск подозрительных файлов в виртуальной среде для поиска подозрительных действий. в этом подходе создается виртуальная среда, в которой запускаются подозрительные файлы для того, чтобы проверить, не являются ли они вредоносными.

При создании современных антивирусных средств машинное обучение обычно используется для улучшения возможностей обнаружения вируса. В то время как традиционные технологии обнаружения основываются на правилах кодирования для обнаружения вредоносных паттернов, алгоритмы машинного обучения создают математическую модель на основе выборочных данных, чтобы предсказать, является ли файл «чистым» или «зараженным». (Данный подход предполагает анализ наблюдаемых экземпляров для двух, созданных вручную наборов данных: один из них включает только вредоносные файлы, второй – только «чистые»).

Алгоритм машинного обучения создает правила, позволяющие отличать «хорошие» файлы от «плохих», без указания того, какие типы шаблонов или фрагментов данных следует искать. Алгоритм продолжает вычислять и оптимизировать свою модель, пока не получит точную систему обнаружения, которая не классифицирует «хорошие» программы как «плохие», а «плохие» – как «хорошие».

Таким образом, поставленная задача может быть решена путем разработки нейронных сетей для создания самообучающейся системы. Такая система работает в адаптивной среде, принимая различные входные данные файла, чтобы определить, является ли он «чистым» или «зараженным» (вредоносным).

Входными данными, рассматриваемыми для обучения нейронной сети, являются различные области структуры Portable Executable-файла (PE – «переносимый исполняемый»). Существенным преимуществом использования этого метода является тот факт, что вся необходимая информация о файле может быть получена без его фактического выполнения.

В машинном обучении сеть обучается, рассматривая подмножество признаков в качестве входных данных для выбранного алгоритма обучения. В основном это связано с тем, что не все признаки являются полезными или актуальными.

Некоторыми из используемых алгоритмов отбора признаков являются:

Критерий соответствия «хи-квадрат» (χ^2) основан на статистической теории. Этот метод измеряет отклонение от ожидаемого распределения, в предположении, что появление признака независимо от значения класса.

Критерий соответствия (χ^2) определяется по формуле (1).

$$\chi^2 = \sum \frac{(P-P_1)^2}{P_1} \qquad (1)$$

P – фактические (эмпирические) данные;

P_1 – «ожидаемые» (теоретические) данные, вычисленные на основании «нулевой гипотезы»;

$\sum$ – знак суммы.

Критерий прироста информации, как следует из этого термина, – это количество информации, полученное при рассмотрении конкретного признака. При

учете признака вычисляется значение энтропии (меры неопределенности признака). Чем меньше энтропия, тем меньше неопределенность, соответственно, имеется больше информации. Критерий прироста определяется как разница между исходной энтропией и ожидаемой апостериорной энтропией после рассмотрения признака.

В регрессионном анализе критерий Фишера (F-тест) позволяет оценивать значимость линейных регрессионных моделей. В частности, он используется в шаговой регрессии для проверки целесообразности включения или исключения независимых переменных (признаков) в регрессионную модель.

В дисперсионном анализе критерий Фишера позволяет оценивать значимость признаков и их взаимодействия.

Критерий Фишера позволяет сравнивать величины выборочных дисперсий двух независимых выборок. Для вычисления F нужно найти отношение дисперсий двух выборок, причем так, чтобы большая по величине дисперсия находилась бы в числителе, а меньшая – в знаменателе. Критерий вычисляется по формуле (2).

$$F = \frac{\delta_x^2}{\delta_y^2} \qquad (2)$$

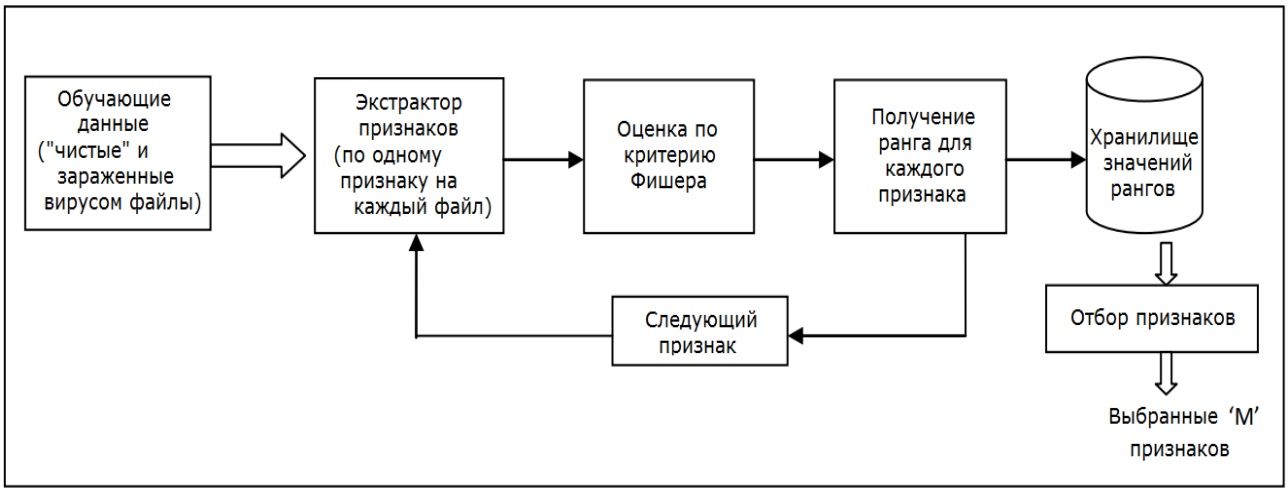
δ_x^2, δ_y^2 – дисперсии первой и второй выборки соответственно.

Преимущество использования нейронных сетей заключается в том, что они обучаются через обучающие данные, обновляют свои веса и дают точные результаты.

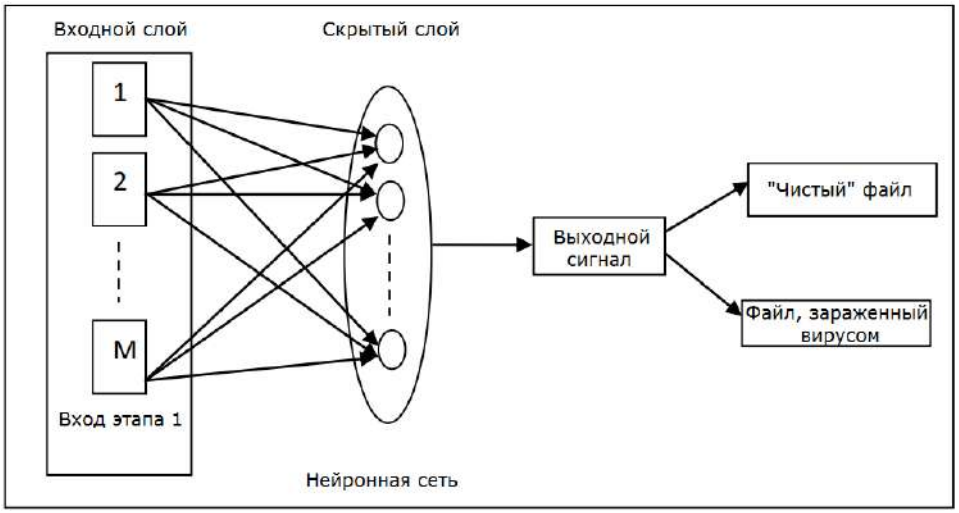
Существует два типа алгоритмов обучения нейронных сетей:

1. Алгоритм обучения с учителем.
2. Алгоритм обучения без учителя.

Разработка системы осуществляется в два этапа. На первом этапе выполняется процедура выбора признаков, принимающая входные данные из файлов, составляющих обучающую выборку:



На втором этапе выполняется обучение нейронной сети, а затем файл классифицируется как «чистый» или как зараженный вирусом:



Выходные данные первого этапа, которые состоят из M наиболее важных признаков, передаются в нейронную сеть в качестве входных данных. Используя эти признаки, нейронная сеть обучается, а затем, когда файл предоставляется в качестве входных данных, она выполняет бинарную классификацию, тем самым, определяет его как «чистый» или как «зараженный вирусом».

Таким образом, несколько наиболее релевантных признаков могут быть отобраны путем применения алгоритма оценки Фишера к данным из структуры PE. Обучая нейронную сеть с помощью множества файлов, можно определить, является ли файл «чистым» или зараженным вирусом. Существенное преимущество, которое дает использование этого метода, состоит в том, что выполнение файла не требуется. Следовательно, эта система может преодолеть недостатки классического антивирусного программного обеспечения, которое полагается на традиционные файлы определений вирусов.

Список литературы:

1. Ашихмина М. В., Городничев В. В., Григоренко А. В. Нейронные сети как основа для разработки антивируса // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов : материалы IV Международной научно-практической очно-заочной конференции, 2016. С. 3–7.

2. Пидченко И. А., Выборнова О. Н. Применение машинного обучения совместно с эвристическим анализом для задач антивирусного сканирования // Математические методы в технике и технологиях. 2020. Т. 5. С. 96–99.

3. Малахов М. А., Мельников Ю. С. Защита конечных точек: антивирусы // Информационные технологии в науке, бизнесе и образовании : сборник трудов XI Международной научно-практической конференции студентов, аспирантов и молодых ученых. 2020. С. 165–170.

4. Кравченко В. О. Обзор методов использования искусственных нейронных сетей в защите информации // Технические науки: проблемы и решения : сборник статей по материалам VII Международной научно-практической конференции, 2018. С. 45–49.

Макеев В. А.[1]**,**
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Плотников Г. Г.,***
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

О ПРИМЕНЕНИЕМ ИСТОЧНИКОВ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ ИНФОРМАЦИОННЫМ СИСТЕМАМ

Актуальность данной проблемы состоит в том, что в современном мире параллельно с довольно быстрым развитием беспроводных систем обращения цифровой информации возрастает изготовление и распространение специализированных технических средств, предназначенных для радиоперехвата, радиомониторинга или же создания помех в целях недопущения передачи какой-либо информации.

И правоохранительные органы, и злоумышленники используют информационные технологии для определенных целей. Первые благодаря им расследуют преступления, анализируют различные данные, доводят информацию до определенного круга лиц. Вторые же могут использовать информационные технологии для саботажей, террористических актов, взлома, утечки информации, причинению значительного ущерба банкам, организациям и т. д.

В данной ситуации шансы поймать преступников очень малы из-за отсутствия материальных следов совершения правонарушения. Также, для скрытности в сети и, соответственно, для защиты действий злоумышленников от детектирования средствами, работающими в открытом эфире, широко применяется генерация помех. Так, для реализации преступных намерений в отношении банкоматов преступники активно используют источники помех сетям сотовой связи кустарного или промышленного производства. Проводимые эксперименты показали эффективность таких средств в отношении систем передачи извещений охранной сигнализации. Но и решение данной проблемы имеет весьма несложную реализацию. Так в городе Елец Липецкой области на одном из объектов Сбербанка России была продемонстрирована двухканальная система передачи извещений Дельта отечественного производства, обеспечившая устойчивый канал передачи в условиях постановки намеренных помех. Дублирование каналов хоть и не дает полной гарантии устойчивой работы канала передачи извещений в условиях активных помех, но обеспечивает существенно более высокий уровень его защиты.

В настоящее время можно заметить, что преступность в сфере информационных технологий только растет. Это дает понять, что методы и средства для совершения противоправных действий в данной сфере стремительно развиваются.

Так, в России число ИТ-преступлений за первые семь месяцев 2021 г. достигло 320 тыс., то есть на 16 % больше, чем за такой же период в прошлом году. Удельный вес зарегистрированных киберпреступлений по последним данным составил 26,5 %.

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации предусмотрено ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ, а в п. 3, объективная сторона закона предполагает нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации [2], или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

К активным угрозам относятся: внедрение программ, которые позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам; действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы); угроза умышленной модификации информации.

Список литературы

1. Волеводз А. Г., Волеводз Д. А. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран // Правовые вопросы связи. 2004. № 1. С. 37–48.

2. Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_law_10699/ (дата обращения: 17.11.2021).

3. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Киев : ТИД “ДС”, 2001. 688 с.

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие: в 2 ч. / [А. В. Аносов и др.]. М. : Академия управления МВД России, 2019. Ч. 1. С. 31.

Назарити А. А.[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Матюнькин Д. А.[2]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Дворянкин О. А.,***
старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

БОРЬБА С ЭКСТРЕМИЗМОМ ПРИ ПОМОЩИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИНТЕРНЕТА

В XXI в. человечество не может представить свою жизнь без информационных технологий интернета.

Люди каждый день пользуются социальными сетями, различными сервисами: общаются, занимаются бизнесом, учатся, а также заказывают продукты питания, товары, работают и решают свои дела удаленно.

В результате значительная часть нашей жизни перешла в интернет пространство, где в последнее время активизировались преступные группы распространяют экстремистские материалы, а также воздействуют на сознание граждан, призывая к радикальным действиям против России.

С учетом изложенного противодействие экстремизму стало одним из приоритетных направлений деятельности МВД России.

Правоохранительные органы в этой связи базируются на действующем уголовном законодательстве.

Так, в Уголовном кодексе Российской Федерации к преступлениям экстремистского характера относят следующие статьи:

– ст. 280 – публичные призывы к осуществлению экстремистской деятельности;

– ст. 282 – возбуждение ненависти либо вражды, а равно унижение человеческого достоинства;

– ст. 282.1 – организация экстремистского сообщества;

– ст. 282.2 – организация деятельности экстремистской организации.

Однако необходимо отметить, что, не смотря на действующее законодательство, в настоящее время данные статьи не всегда можно полноценно и эффективно применить, так как деяния экстремистского характера очень часто совершаются в информационно-телекоммуникационном пространстве, в частно-

сти в интернете, и в большинстве случаев остаются не раскрытыми по ряду причин.

Одной из них является высокая анонимность в сети Интернет, обеспечивающаяся благодаря большому количеству приложений и информационных технологий. В результате сотрудники правоохранительных органов часто сталкиваются с проблемами установления личности и идентификация лица, занимающегося экстремистской деятельностью.

Самым популярным средством сокрытия личности злоумышленника является технология (сервис) «Tor». Это программное обеспечение находится в свободном доступе и позволяет устанавливать анонимное защищенное сетевое соединение (луковичное соединение) и представляет собой сеть виртуальных туннелей, в которых передается информация в зашифрованном виде.

С помощью этого приложения можно зайти в сегменты Интернета, которые скрыты от общего пользования. Кроме этого есть сайты и форумы, где злоумышленники призывают к радикальным действия против религиозного, государственного и социального строя, организуют незаконные сообщества и организации.

Также используются такие технологии анонимности как VPN.

VPN – это обобщенное название технологий, позволяющих пользователю использовать в интернете не свое, а подменное местоположение, т. е. тем самым, защищая информацию о себе от лишнего внимания.

Эта настройка, включив которую можно просматривать веб-сайты без опасности быть отслеженным кем-либо. Именно поэтому такая технология является проблемной для правоохранительных органов – она усложняет поиск и обнаружение местоположения злоумышленников.

Существует еще одна проблема сокрытия каких-либо данных от правоохранительных органов – это мессенджеры, которые шифруют данные.

Нижеприведенные мессенджеры используют сквозное «end – to–end» шифрование, то есть отправляют зашифрованные сообщения, которые может расшифровать только получатель. Каждое из этих приложений имеет свои преимущества и уникальные особенности.

Signal – платформы: Android, iOS, Windows, Mac, Linux. Signal.

Это приложение поддерживает отправку файлов, групповые чаты, видеозвонки и не уступает по базовым возможностям более популярным и менее безопасным конкурентам. Сейчас Signal используют в WhatsApp и Facebook Messenger, но эталонная реализация этого протокола одноименный мессенджер.

Wire – платформы: Android, iOS, Windows, Mac, Linux, Web.

Мессенджер создан на базе модифицированного протокола Signal для корпоративных клиентов, но его можно использовать и для личных целей.

Threema – платформы: Android, iOS, Web.

Threema – мессенджер, который использует швейцарское правительство. Все данные, которые передает Threema (сообщения, звонки, мультимедийные файлы и даже статусы контактов), шифруются на пользовательских устройствах.

При условии, что этот мессенджер централизованный, его сервер выступает как коммутатор: сообщения проходят через него, но не хранятся там постоянно.

Приведенные примеры приложений могут позволить правоохранительным органам более эффективно противодействовать экстремизму в Российской Федерации.

В заключение хотим отметить, что органам внутренних дел необходимо и важно использовать технологии, которые используют экстремистские организации, но только против них самих, а также эффективно и результативно идти в ногу со временем и информационными технологиями Интернета, но и опережать их в своем развитии.

Список литературы

1. Женское участие в терроризме: религиозный женский опыт или женская дискриминация? // URL: https://cyberleninka.ru (дата обращения: 05.12.2021).

2. Экстремизм с женским лицом, или как современный феминизм толкает человечество в пропасть (информационный портал) // URL: http://katyusha.org (дата обращения: 05.12.2021).

3. Феминизм – это не борьба за равные права // URL: https://rusdozor.ru (дата обращения: 05.12.2021).

4. С глазу на глаз. 7 мессенджеров для приватной переписки // URL: https://club.esetnod32.ru/articles/analitika/s-glazu-na-glaz/ (дата обращения: 05.12.2021).

Чужакова Е. А.[1]*,*
курсант 282 взвода факультета подготовки сотрудников полиции
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Пушкарев В. В.****,*
доцент кафедры предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ: СОСТОЯНИЕ, ВЫЯВЛЕНИЕ И РАССЛЕДОВАНИЕ

Согласно отчетам Европола, практическая деятельность многих стран обращена к проблеме роста активного использования цифровых активов в противоправных целях в даркнете – далее). По аналитическим данным Chainalysis лидерами по объемам криптовалютных транзакций в даркнете по итогам 2020 г. стали Россия, США и Украина (4 и 5 места заняли Китай и Вьетнам). Общий объем входящих и исходящих транзакций составил 1,7 млрд долл. (в Российской Федерации – 288 млн долл., в США – 179 млн долл., в Украине – 98 млн долл.). Полагается, что подавляющая часть платежей в России и Китае, полученная черным рынком, задействована в отмывании денежных средств [1]. Отмечается активное использование криптовалютных бирж, p2p-платформ и сервисов микширования в целях сокрытия фактов противоправных действий. Несомненно, что цифровой и анонимный механизм криптовалюты способствуют росту онлайн-рынков на даркнете, где торгуют незаконными товарами и услугами.

Данные показатели свидетельствуют об усилении позиций преступных организаций, использующих цифровые финансовые активы (далее – ЦФА) для достижения преступных замыслов, отмывания доходов и финансирования терроризма (далее – ОД/ФТ).

Помимо незаконной торговли, оплаты услуг, операций по конвертации валюты, криптовалюты стали удобным инструментом для финансирования террористической деятельности. Терроризм – одна из опаснейших угроз современного мира, и совершенствование способов обеспечения деятельности радикальных группировок способствует нарастанию мощностей криминального сообщества.

В этом аспекте высказался Яйя Фаньюзе, директор политического анализа в Фонде защиты демократии Центра по санкциям и незаконному обороту финансов, отметив, что террористические группы стали активно использовать цифровую валюту для сбора средств, а первой из таких группировок отмечена Ibn Taymiyya Media Center, ITMC (пропагандистское подразделение интернет-джихадистов в секторе Газа) [2].

Весомую долю в финансировании терроризма имеют доходы от наркотрафика, в частности, из стран Юго-Восточной и Южной Азии, незаконного обо-

рота оружия, транспортировки нелегальных мигрантов из стран Северной Африки, Ближнего Востока, Афганистана.

Финансирование терроризма направлено на способствование совершению террористических актов, вооруженных мятежей, созданию незаконных вооруженных формирований, захвата заложников и др.

В 2020 г. Вейт Бюттерлин, эксперт по финансовым преступлениям, который проводил расследования в более чем 20 странах и который был похищен в ходе одного из расследований, объяснил в интервью CNN, что борьба с финансированием терроризма будет постоянной проблемой. Он отметил, что 10 крупнейших террористических организаций мира имеют, по оценкам, годовой бюджет в размере 3,6 миллиарда долларов США [3].

По информации ABC News, в сентябре 2020 года группой Министерства экономики Франции Tracfin была раскрыта сложная схема финансирования терроризма, и в ходе проводимой полицией Франции операции были задержаны 29 человек (от 22 до 66 лет), подозреваемые в причастности к данной незаконной деятельности [4]. Также, в октябре 2021 года по подозрению в участии в запрещенной в России террористической организации «Исламское государство» в Вологде был задержан мужчина 1991 года рождения, ранее судимый за преступления террористической направленности. По данным пресс-службы Вологодского Управления ФСБ, задержанный установил связи с террористической организацией и организовал сбор средств в криптовалюте для финансирования ИГ, создав закрытые группы в Telegram. Кроме того, он занимался онлайн-обучением террористов технологиям анонимизации в сети и соблюдению конспирации. В отношении жителя Вологды возбуждены уголовные дела по ч. 2 ст. 205.5 (участие в деятельности террористической организации) и ч. 1.1 ст. 205.1 (финансирование терроризма) УК РФ [5].

Заместитель секретаря Совета безопасности России Юрий Коков в рамках интервью «Российской газеты» заявил о наращивании террористами своих финансовых мощностей: «Так, по оценкам экспертов ООН, финансовые резервы ИГИЛ (запрещенная в Российской Федерации группировка «Исламское государство») составляют до 300 млн долл. Наряду с этим террористы продолжают искать новые источники финансирования» [6].

Процесс финансирования терроризма состоит из трех основных этапов:

– привлечение средств как законным, так и незаконным путем;

– перемещение полученных средств (задействование законных и незаконных механизмов);

– использование средств для обеспечения террористической деятельности.

Перемещение средств может быть реализовано в том числе и с использованием альтернативных систем платежа, статус и легальность использования которых на данный момент не урегулированы. Альтернативные платежные системы функционируют вне государственной системы контроля и надзора, выпадая из-под юрисдикции государства. Путем использования виртуальной валюты преступники могут осуществлять крупные денежные переводы в обход традиционных финансовых систем. В этой связи требуется законодательная проработка вопросов совершения финансовых операций, находящихся вне ра-

мок требований Федерального закона от 7 августа 2001 г. № 115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – ФЗ-№ 115) [7].

Причины использования виртуальных валют в процессе отмывания доходов и финансирования терроризма:

1. Высокий уровень анонимности.
2. Экстерриториальность (криптовалютные кошельки не привязываются ни к физическому адресу, ни к конкретному лицу).
3. Децентрализованный характер операций.
4. Конвертируемость криптовалюты.
5. Малая стоимость и простота использования.
6. Повсеместная доступность платежных систем и скорость совершения операций.

Основной аспект в выборе преступниками криптовалюты – степень защищенности для самих субъектов ее использования от нежелательного вмешательства и деанонимизации личности, что достигается использованием «миксеров», «темных кошельков», сети Tor и других инструментов.

Помимо положительных моментов, стоит также отметить ряд рисков, с которыми могут столкнуться преступники:

1. Непостоянный курс криптовалюты.
2. Возможность взлома криптокошелька и доступа к средствам.
3. Сложность нахождения надежной системы для конвертации фиатных денег в криптовалюту.
4. Совершенствование методов отслеживания движений криптовалюты, используемых в деятельности правоохранительных органов.

Заместитель директора Федеральной службы по финансовому мониторингу Герман Негляд заявил, что наибольшей популярностью у преступников обладают такие криптовалюты, как Bitcoin, Ethereum и Monero. Росфинмониторинг совместно с подразделениями финансовых разведок иностранных государств занимается фиксацией фактов использования цифровых активов, выявляя признаки противоправной деятельности (заключено порядка 100 международных соглашений по данному аспекту) [8].

К числу государственных органов, компетентных в вопросах ПОД/ФТ, относятся: Роскомнадзор, Пробирная палата Российской Федерации, Банк России, Росфинмониторинг. Правовой основой вышеуказанной деятельности является ряд международных и национальных актов (международные конвенции, резолюции СБ ООН, документы ФАТФ, Федеральные законы Российской Федерации, Указы Президента Российской Федерации, соответствующие документы Минфина, ФСФР России, ЦБ России и др.).

Финансовое расследование в сфере ПОД/ФТ, по своей сути, представляет собой изучение финансовых элементов деятельности субъектов экономических отношений с целью выявления признаков противоправной деятельности.

Финансовое расследование включает в себя несколько этапов:

1. Сбор данных.
2. Обработка полученных данных.

3. Аккумулирование аналитических сведений.

4. Выявление признаков ОД/ФТ.

5. Возбуждение в установленном законом порядке уголовного дела.

На каждой стадии расследование подлежит строгому государственному контролю.

Сложность расследования дел по ОД/ФТ с использованием криптовалют объясняется следующими особенностями:

– отсутствие необходимой законодательной базы, регулирующей функционирование криптовалюты;

– сложность процедуры отслеживания отправителя и получателя денежных средств;

– отсутствие системы превентивных мер в данной области;

– необходимость обращения к сторонним источникам для получения финансовой информации.

Для успешного и полноценного проведения расследования необходимо привлекать высококвалифицированных IT-специалистов, так как органы предварительного расследования должны располагать криминалистически значимыми сведениями о движении криптовалюты, произведенных транзакциях, особенностях платежной системы.

В преступлениях, в которых криптовалюта выступила средством (инструментом) совершения преступления, определяющее значение имеет установление обстоятельств, относящихся к осуществлению конкретных транзакций: события преступления (время, место осуществления операции), лица (стороны перевода), информация о платежной системе, реквизиты кошельков, вид и размер переведенной криптовалюты [9]. Определение времени совершения транзакции затрудняется наличием внутренних систем компьютеров, которые фиксируют время операции в разных часовых поясах и различных программных кодах. А фактическое местоположение физического лица, осуществившего перевод, может не совпадать с местонахождением программного оборудования. Проблема установления личности связана с невозможностью установления принадлежности криптокошелька и связи биткоин-адреса с обменниками, биржами, миксерами и др. Также стоит остановиться на том, что в России на данный момент криптовалюта не имеет правового режима (поскольку у виртуальной валюты нет своего правового статуса, она не может являться имуществом), что создает определенную проблему в отнесении ее к какому либо процессуальному элементу (ее нельзя признать ни предметом посягательства, ни средством/орудием совершения преступления). Необходимо обратиться и к вопросу закрепления правового статуса «цифровых доказательств», которые могут быть использованы в следствии и в суде как законное, допустимое доказательство по делу.

Поэтому, несмотря на то что все сведения о транзакциях хранятся в блокчейне в открытом доступе, добыть криминалистически значимую информацию невозможно без применения специальных знаний в области IT-технологий и понимания механизма функционирования криптовалюты. В России для отслеживания производимых транзакций, содержащих признаки противоправной

деятельности, Росфинмониторингом совместно с МВД России и РАН был разработан национальный сервис «Прозрачный блокчейн», способный отслеживать и фиксировать движения криптовалюты и определять конечного бенефициара. К сожалению, данный программный комплекс позволяет отследить только транзакции биткоина, таким образом, в криминальной сфере наблюдается отказ от использования данной криптовалюты на этапе подготовки и совершения преступлений. Внимание преступников переключается на более анонимные криптовалюты: ZCash, Monero, Dash и другие.

Согласно ст. 3 ФЗ-№ 115 уполномоченный орган осуществляет контроль за операциями с денежными средствами и иным имуществом, основываясь на информации, которую предоставляет ему организация, осуществляющая такие операции. Так, встает вопрос о законодательном закреплении возможности и обязанности провайдеров криптовалютных платежей предоставлять информацию и блокировать аккаунты по запросу компетентного органа.

Таким образом, объединение усилий и тесное сотрудничество различных государственных структур и служб, диалог с религиозными лидерами мусульманских организаций и совершенствование методик финансового расследования должно быть направлено на снижение темпов радикализации террористической деятельности и противодействие финансированию терроризма.

Цифровое пространство стало удобной платформой для оперативного управления рассредоточенными силами и средствами, в том числе финансовыми активами. Рост террористической и экстремисткой активности становится серьезнейшей угрозой национальной безопасности, а расширение географии воздействия и распространение деструктивной идеологии способствует развитию и пополнению рядов организованной преступности.

В этом аспекте перед государственными органами стоят следующие задачи:

– создание регулирующего законодательства и иных норм, определяющих функционирование криптовалюты в рамках правового поля Российской Федерации;

– урегулирование вопросов международного сотрудничества в расследовании преступлений, связанных с ОД/ФТ с использованием криптовалюты;

– разработка методических рекомендаций по организации расследования и раскрытия данной категории преступлений;

– проработка следственной и судебной практики.

Обучение сотрудников правоохранительных органов методикам расследования преступлений, совершаемых с использованием криптовалюты, в том числе методикам ПОД/ФТ [10].

Целесообразно продолжение мониторинга развития событий в данной области силами неформального форма «Группы двадцати» (членом которой является Российская Федерация) совместно с Группой разработки финансовых мер борьбы с отмыванием денег (далее – ФАТФ).

Список литературы

1. Chainalysis Insights // URL: https:// blog.chainalysis.com/ (дата обращения: 28.10.2021).

2. ABC News. Сайт новостного подразделения Walt Disney Television // URL: https://abcnews.go.com (дата обращения: 29.10.2021).

3. CNN. WarnerMedia // URL: https:// www.cnn.com.

4. Bits.media // URL: https://bits.media/ (дата обращения: 29.10.2021).

5. Пресс-служба Управления Федеральной службы безопасности Российской Федерации по Вологодской области // URL: http://www.fsb.ru/ (дата обращения: 07.11.2021).

6. Интервью заместителя секретаря Совета безопасности России Юрия Кокова // Российская газета. 2019. № 230 (7988).

7. Федеральный закон Российской Федерации от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СПС «КонсультантПлюс». URL: http:// www.consultant.ru (дата обращения: 25.10.2021).

8. Культовый журнал о биткоине, технологии блокчейн и цифровой экономике // URL: https://forklog.com/ (дата обращения: 28.10.2021).

9. Надысева Э. Х. Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности. 2019. № 3. С. 223–227.

10. Информационное письмо Банка России от 14 августа 2018 г. № ИН-014-12/54 «О национальной оценке рисков ОД/ФТ» (вместе с «Публичным отчетом. Национальная оценка рисков легализации (отмывания) преступных доходов. Основные выводы 2017–2018», «Национальной оценкой рисков финансирования терроризма. Публичный отчет 2017–2018») // СПС «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 25.10.2021).

11. Противодействие преступлениям в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Макаров Р. Е.[1]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Золоторев Д. В.[2]***,***
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Дворянкин О. А.,***
старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ЖЕНСКИЙ ФЕМИНИЗМ КАК ИСТОК БУДУЩЕГО ТЕРРОРИЗМА

Современный мир развивается с невероятно высокой скоростью и то, что раньше считалось нормой, сейчас же приобретает новый вид.

В 1940 г. французский философ и социолог Шарлем Фурье ввел термин феминизм. Первыми представителями этого направления считают женщин Афру Бенн (1640–1689) и Мэри Эстел (1666–1731).

Первоначальная суть этого движения предполагала борьбу за предоставление женщинам тех же прав и свобод, которыми были наделены мужчины. Например, за избирательное право. Первая американская феминистка Абигейл Смит-Адамс вошла в историю со следующей фразой: «Мы не станем подчиняться законам, в принятии которых мы не участвовали, и власти, которая не представляет наших интересов».

Развитие феминизма в России началось в 1812 г., когда было создано Женское патриотическое общество. Чуть позже его участницы стали известны как «жены декабристов». Позже активными русскими женщинами был создан ряд общественных организаций филантропического и образовательного характера.

Феминизм и терроризм на первый взгляд разные явления, но если вернуться на несколько десятилетий назад, то можно увидеть, что ростки женского терроризма выросли на почве борьбы за права и свободы женщин. Возникшая под влиянием повышения уровня образованности женщин и возможности зарабатывать себе на жизнь, протест против зависимости от мужчин, идея полного равноправия с ними, а также обостренное чувство справедливости в ее женском понимании, привели часть революционерок к участию в террористических актах.

Для того чтобы привлечь внимание к своим новым женским проблемам – освоению мужского образа жизни, требованию полного равноправия вплоть до отождествления себя с мужчинами, часть активисток женского движения становилась на путь физического самопожертвования, стремления своей смертью привлечь внимание власти к социальным, прежде всего женским проблемам, что неизбежно стало приводить их к террористической деятельности.

Первоначально это были представительницы аристократии и буржуазии, получившие высшее образование, но уже к началу XX в. к ним стали присоединяться и женщины из низших, малограмотных слоев населения. Довольно скоро террористки стали иметь более высокий образовательный уровень, нежели террористы-мужчины.

Желая походить на мужчин, женщины стали не только носить мужскую одежду, заниматься мужскими профессиями и мужскими делами, но и активно участвовать в политической жизни.

Если не знать истории женской эмансипации можно удивляться тому, почему сегодня женщины во многих странах мира активно участвуют в политических движениях и в том числе в терактах. Но если вспомнить, что первые террористки появились в России в конце XIX – начале XX в., т. е. тогда, когда женщины получили доступ к высшему образованию и вступали в политические партии, то такая связь становится очевидной. Ради стремления жить как мужчины, участвовать в политической жизни страны, они готовы отказаться от своей женской природы – мягкости, терпеливости, боязненности, покорности и становиться агрессивными, нетерпимыми, нередко по жестокости превосходя мужчин.

В результате участия в террористической деятельности в годы революции и гражданской войны женщины добились своей цели – официального признания равенства с мужчинами на государственном и международном уровнях, что привело не только к возможности получения высшего образования, но и к занятию должностей в партийных и правительственных органах. В связи с этим террористическая деятельность женщин в нашей стране и странах западного мира прекратилась, были достигнуты на тот период времени должные результаты.

Однако феминистки не прекратили свою борьбу с мужчинами, поставив перед собой новую цель – скинуть их с пьедестала и встать на него самим.

Одним из распространенных мотивов террористической активности женщин считается их моральная и психическая патология, неравноценность мужских и женских черт, что приводит к обвинениям в женской несостоятельности.

Исследователи при объяснении женского терроризма говорят о том, что к террору как осмысленному выбору женщина может прийти, посчитав достойным данный способ самоутверждения. Поэтому женщины, как правило, глубоко уверены в необходимости и оправданности совершения терактов.

Нарастание женского терроризма обусловлено подъемом феминистского движения, способствовавшего пониманию женщинами своей значимости,

и возможностью самореализации в различных сферах деятельности, в том числе и в терроризме.

В современном мире, феминизм также все ближе подходит к терроризму. Идеи борьбы за равенство женщин уже устарели, но борьба с мужчинами продолжается. И благодаря всемирной сети Интернет, данный способ набирает все большую популярность среди участниц данного направления. Потому что, это самый простой метод вербовки масс, так как огромное количество людей ежедневно используют данную сеть в своей повседневной жизни. Сейчас же феминизм строится на дискриминации и борьбе именно с мужчинами, попытками унижения другого пола, возвысить свой статус в обществе. Существует большое количество сообществ в социальных сетях, которые распространяют идею радикального феминизма.

Также была создана петиция за приравнивание феминизма к терроризму. Автором данной петиции является активистка Джэнет Уилкинсон из Испании. Она считает, что «На протяжении многих лет феминизм оказывал давление на мужчин и женщин, которые просто хотели жить своей жизнью. Нередко этот пресс перерастал в физическое воздействие на мужчин». Уилкинсон также призвала запретить курсы для женщин, где им «промывают мозги», заставляя считать себя жертвами. Петиция собрала 14 264 подписи, но в настоящее время «по определенным причинам» петиция удалена.

Таким образом, все чаще феминизм становится не просто борьбой за права женщин, а борьбой с противоположным полом. Изначально феминизм имел благородные цели, так как, в прежнее время, права женщин действительно были сильно ущемлены. Сейчас же данный термин воспринимается с отрицательной стороны, причем не только мужчинами, но и женщинами. Феминизм в современном мире воспринимается как война с мужским полом.

В заключение считаем целесообразным сказать, что дальнейшее развитие этого движения угрожает общественной безопасности. Борьба за права выходит за рамки допустимого, сторонники этого движения все чаще прибегают к террористским действиям. В настоящее время проблема женского терроризма приобретает новые формы и иные масштабы, а мотивами служат идеи вознесения женщин в обществе.

Список литературы

1. Женское участие в терроризме: религиозный женский опыт или женская дискриминация? // URL: https://cyberleninka.ru (дата обращения: 05.12.2021).

2. Экстремизм с женским лицом, или как современный феминизм толкает человечество в пропасть // URL: http://katyusha.org (дата обращения: 05.12.2021).

3. Феминизм – это не борьба за равные права // URL: https://rusdozor.ru (дата обращения: 05.12.2021).

Наумов Е. Е.[1]*,*
курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Пименова О. В.****,*
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК УГРОЗА БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Принято разделять угрозы безопасности критической информационной инфраструктуры (далее – КИИ) на две большие группы: внешние и внутренние. Внешние угрозы представляют собой действия отдельных людей и организаций, которые находятся вне критических информационных объектов (далее –КИО). Как правило, данную разновидность угроз создают различные террористические и хакерские группировки, в том числе различные хакерские группировки, поддерживаемые государствами. Внутренние угрозы – это различные ошибки и неправомерные действия персонала КИО и его системы безопасности.

Из всех видов угроз особую роль играет человеческий фактор, особенно как разновидность внутренних угроз. Человеческий фактор проявляется в действиях персонала КИО, которые потенциально могут привести к опасным последствиям. Данный тип угроз трудно поддается анализу причин, которые могут привести к совершению сотрудником противоправных действий, как намеренных, так и нет (злоумышленных действий и непреднамеренных ошибок). Это обуславливается множеством различных условий и факторов, которые могут влиять на принятие решений человеком, и неоднозначностью между причинами и действиями. Также при учете рисков стоит отслеживать и учитывать изменчивость данных факторов.

Учитывая современные реалии, данную тему стоит рассматривать в первую очередь с точки зрения информационной безопасности КИО. Это обусловлено тем, что с конца XX в. количество атак с использованием компьютерных технологий постоянно увеличивается.

Наиболее громким и известным случаем нарушения безопасности КИИ, связанным с человеческим фактором, является нарушение работы урановых центрифуг на иранском заводе в Натанзе. В 2008 г. израильским и американским спецслужбам удалось заразить флеш-накопитель одного из сотрудников Siemens червем Stuxnet. Работник нарушил технику безопасности, подключив

накопитель к одному из служебных компьютеров, чем вызвал заражение изолированной сети. Червь перехватил управление центрифугами по обогащению урана и заставил их работать на полной скорости, в то время как на мониторах инженеры не наблюдали каких-либо аномалий в работе системы. В итоге было поражено 1368 из 5000 центрифуг. Данная атака по мнению большинства экспертов сильно повлияла на ядерную программу Ирана, так как сроки запуска новой ядерной АЭС в Бушере были сорваны. Этот пример наглядно демонстрирует насколько важно минимизировать человеческий фактор в осуществлении безопасности КИИ.

Изолирование информационных систем снижает вероятность их заражения и позволяет исключить внешние угрозы. Однако система все еще уязвима перед внутренними угрозами. В приведенной выше истории самым простым вариантом проведения атаки на объект было использование человеческого фактора, а именно безответственности и пренебрежения техникой безопасности. Таким образом, система, выглядевшая на первый взгляд защищенной, стала жертвой банальной человеческой беспечности.

Подобные атаки совершаются ежегодно и их количество продолжает расти. Помимо государственных объектов, атаке подвергается промышленность крупных компаний. Например, согласно отчету компании Positive Technologies за 2020 г., количество атак на промышленность в 2020 г. увеличилось по сравнению с прошлым годом на 91 %. В то же время доля атак на критические информационные объекты с помощью социальной инженерии в 2019 и 2020 гг. составляла 84 % и 74 % соответственно [1]. Это говорит о том, что наименее защищенным элементом КИИ является персонал.

Факторы, совокупность которых представляет собой человеческий фактор, подразделяются на две группы: относящиеся к управлению (рабочая нагрузка и некачественная работа персонала) и связанные с конечным пользователем.

Среди множества различных факторов можно выделить несколько, способных оказывать сильное влияние на поведение сотрудников:

1. Недостаток мотивации. Многие организации считают, что сотрудников необходимо мотивировать на безопасное поведение с информационными активами, и руководство должно быть в состоянии определить, что мотивирует их персонал.

2. Недостаток осведомленности. Большая часть персонала критических информационных объектов не обладает достаточным количеством общих знаний об атаках. Наиболее часто встречаемые примеры неосведомленности могут быть следующими: пользователи не умеют определять шпионское программное обеспечение и не обладают пониманием того, как важно указывать надежный пароль. Сотрудники зачастую не могут защитить себя от кражи личных и корпоративных данных, а также как контролировать доступ других пользователей к их компьютеру.

3. Убеждение. Распространенными примерами рискованного убеждения являются ложное представление пользователями, что установка антивирусного программного обеспечения решает все их проблемы по защите информации. Помимо того, что существует множество других путей утечки информации, наличие антивируса не дает полной безопасности, в связи с возможной новизной вредоносного программного обеспечения, используемого при атаке, которое не опознается антивирусами.

4. Неграмотное пользование технологиями. Даже самая лучшая технология не может преуспеть в решении проблем информационной безопасности без непрерывного человеческого сотрудничества и эффективного использования этой технологии. Результатом ненадлежащего использования технологий могут являться несанкционированное изменение конфигурации систем, получение доступа к паролям других сотрудников, получение недопустимой информации. [2] Поэтому организациям следует всегда продуманно и четко внедрять технологии.

Вышеприведенные факторы зачастую приводят к тому, что сотрудники могут совершать ошибки и частично не выполнять требования техники безопасности, чем создают слабые места в защите КИО. Данные действия персонал совершает по небрежности или легкомыслию. Однако хакеры способны сами провоцировать ситуации, в которых вынуждают сотрудников выполнять действия, приводящие к нарушению безопасности КИО. Для этого злоумышленники используют методы социальной инженерии.

Социальная инженерия – это психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации [3]. Наиболее часто используемые виды атак с использованием социальной инженерии:

1. Использование «приманки» или «дорожное яблоко». Злоумышленник оставляет зараженный флеш-носитель на видном месте. Сотрудник находит его и вставляет в служебный компьютер. В результате вредоносное ПО может проникнуть в изолированную сеть или даже само устройство вызовет поломку в компьютере.

2. Претекстинг. Это действия злоумышленника, отработанные по заранее спланированной схеме (претексту). В результате жертва должна совершить определенное действие, или выдать нужную информацию.

3. Фишинг. При фишинговой атаке жертва получает сообщение от источника, который на первый взгляд кажется достоверным, о просьбе выдать определенную служебную информацию.

4. Quid pro quo (кто вместо кого). Злоумышленник, притворяясь сотрудником технической поддержки, осуществляет прозвон случайных номеров организации на наличие технических проблем. При их наличии предлагает выполнить ряд команд, которые позволят злоумышленнику запустить вредоносное ПО.

5. Троянский конь. Злоумышленник отправляет жертве письмо по электронной почте с вложением, содержащим файл, содержание которого потенциально может ей быть интересно. Жертва открывает файл и на любое устройства попадает вредоносное ПО.

Существует множество других видов атак с использованием социальной инженерии, но во всех случаях, рассматриваемых мной, целью является заражение внутренней сети КИИ. Злоумышленник перечисленными способами либо получает служебную информацию необходимую для дальнейших атак, либо добивается заражения.

Самый основной способ защиты от социальной инженерии – это обучение сотрудников, повышение их осведомленности в вопросах информационной безопасности. Незнание не освобождает от ответственности. Все сотрудники должны знать о негативных последствиях нарушения безопасности КИИ.

Список литературы

1. Positive Technologies. Актуальные киберугрозы: итоги 2020 года // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-/#id8 (дата обращения: 22.11.2021).

2. Habr. Человеческий фактор в информационной безопасности // URL: https://habr.com/ru/post/344542/ (дата обращения: 23.11.2021).

3. Wikipedia. Социальная инженерия // URL: https://ru.wikipedia.org/wiki/ Социальная_инженерия (дата обращения: 24.11.2021).

Миляев Г. А.[1]**,**
курсант факультета подготовки сотрудников
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель: ***Лустин В. И.,***
старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕЗАКОННОГО ИНФОРМАЦИОННОГО ВМЕШАТЕЛЬСТВА

В современном мире каждый человек находится в зависимости от информационных технологий. Вследствие этого появляется необходимость в охране и защите информации от взлома и кражи. Рассмотрим несколько вариантов криптографической защиты информации при обмене данными.

В данный момент в криптографии используется два основных метода шифрования, классифицирующиеся по типу ключей: симметричное и ассиметричное.

Симметричное шифрование. [1]

В данном алгоритме для шифрования и дешифрования используется один и тот же секретный ключ, что и является его главной особенностью, потому что скорость дешифрации сообщения довольно быстра и это упрощает процесс обмена данными. По этой причине симметричное шифрование часто используется вместе с ассиметричным шифрованием для более высокой эффективности, то есть весь процесс шифрования разбивается на части, каждая из которых шифруется своим методом. Из минусов можно отметить то, что чем дольше идет использование ключей при общении пользователей, тем легче взломать сам этот ключ, то есть легче понять способ шифрования сообщений между определ енными пользователями.

Ассиметричное шифрование [2].

Говоря об ассиметричном шифровании нужно отметить то, что в основном он используется для шифрования небольших массивов данных, так как основной операцией в них является возведение больших чисел в степень. Суть данного алгоритма заключается в том, что пользователи должны создать по открытому и закрытому ключу для каждого. Одним из лучших способов создания ключей является RSA алгоритм. Благодаря ему, ключи становятся математически зависимыми друг от друга. То есть открытый ключ служит для шифрования информации, а закрытый для дешифрации и получения исходного сообщения, но расшифровать сообщение может только тот, кто получает сообщения. Одной из особенностей ключей, является то, что из открытого ключа нельзя получить закрытый и наоборот. Сам алгоритм подразумевает, что клиенты сначала обмениваются публичными ключами, затем один из клиентов шифрует информацию публичным ключом другого, а второй уже дешифрует его своим закрытым ключом. В случае если значения не буду сходиться, то пользователи поймут,

что их данные хотят перехватить и могут прервать общение. На ассиметричном шифровании работают все сайты на HTTPS протоколе, а также электронные сообщения по протоколу PGP.

Следующими методами защиты являются алгоритмы хэширофания, применяющиеся для решения наиболее важных проблем, как обеспечение целостности и причастности на всех этапах документооборота, а также вопросы использования различных хэш-фукций в системах обработки информации.

Хэш-функции [4].

Хэш-функции создают уникальный цифровой отпечаток и представлют собой функцию, которая переводит исходные данные в хешированный вид, и в часто используется для шифрации паролей при регистрации на различных интернет ресурсах. Этот вид используется для паролей пользователей социальных сетей. Одним из ключевых плюсов данного метода является то, что это функция однонаправленная, то есть если взять данные, перевести их через хэш-функцию и попробовать сделать обратную операцию, то ничего не выйдет. Зная значение хэша, очень тяжело получить исходную информацию. Это обусловлено тем, что ещ е нет эффективного алгоритма, позволяющего просто перевести хэш в исходное значение за приемлемый отрезок времени. Из плюсов следует отметить то, что эта функция всегда будет иметь уникальный хэш. Данный факт можно аргументировать наличием лавинного эффекта. К примеру, если из исходных данных заменить 1 какой-либо элемент, то значение хэша кардинально измениться и никак не будет совпадать с предыдущим значением. В случае одинаковых паролей, появляется Дополнение – строка данных, пропускаемая через хэш-функцю, вместе с паролем, что дает уникальный хеш для одинаковых паролей. Быстрая скорость вычисления хэша из любого сообщения – это еще один положительный факт, но это и является одной из уязвимостей. Злоумышленники могут этим воспользоваться и перебрать пароль с помощью bruteforce атаки, осуществляемые с помощью программ и расширений на ПО Kali Linux и найти исходные данные путем простого перебора всех возможных значений. [5] Ещ е одним плюсом является практически полное отсутствие коллизий – результат не может стать одинаковым для двух разных данных. Однако, есть большое замечание, если злоумышленники взломают базу данных и получат доступ к хэшам паролей, то могут использовать коллизию в корыстны целях. Это осуществляется с помощью таблиц, где заранее просчитаны хэши для определенных простых слов-паролей. Еще можно отметить то, что размер получаемого значения хэша всегда будет фиксируемым, то есть будет из определенного количества символов.

Таким образом, эффективность хэш-функций является приемлемой для использования, несмотря на небольшие минусы.

Электронная подпись [6]

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.[7]

Она аутентифицирует электронные сообщения и письма, то есть подтверждает личность отправителя и подлинность его сообщения. Данный алгоритм может работать на симметричном шифровании, где используется участие третьего лица, то есть арбитра. Проблема данного способа в доверии к арбитру, так как им может быть злоумышленник. Так же ЭП работает на ассиметричном шифровании, который используется чаще, чем симметричный.

Этот метод работает несколько иначе, закрытый ключ используется для шифрования данных, а открытый для дешифрации. Помимо всего, здесь задействованы хэш-функции, которые используются на этапе шифрования и дешифрования. То есть после получения данных, второй пользователь сравнивает изначальное и конечное значения хэша, то значит, что операция удалась.

Еще одним плюсов является использование электронных сертификатов в процессе создания электронной подписи. Они позволяют удостоверить данные о владельце. Зачастую используются децентрализованные сертификаты, которые выдаются и поддерживаются сертификационными центрами, список которых указан на сайте Министерства цифрового развития, связи и массовых коммуникаций. Здесь можно отметить плюс данной схемы, так как подделать электронную подпись крайне тяжело. К примеру, есть пара типов атак для получения ЭП.

Коллизия второго ряда – осуществляет подделку двух документов с одинаковой подписью и в нужный момент преступник заменяет один документ другим. На практике это очень сложно, но возможно благодаря недочетам отдельных алгоритмов в хэшировании и подписях.

Социальная атака – направлена на манипуляции с закрытыми и открытыми ключами. К примеру, злоумышленник может выдавать себя за владельца, подменив его открытый ключ своим.

Но, несмотря на незначительные пробелы в защите, ЭП является одним из самых надежных методов сертификации и шифрования документов, из-за того, что используется надежный посредник, зачастую которым являются государственные сайты и системы.

Подводя итоги, проблема конфиденциальности и защиты информации будет актуальна всегда, потому что каждый день совершенствуются методы и алгоритмы защиты информации, но также постоянно создаются новые способы е е кражи. Таким образом, правоохранительные органы должны четко следить за ситуацией, разрабатывать и совершенствовать методы защиты как собственной информации, так и публичной информации чтобы не допустить больших утечек, краж и дальнейшей продажи.

Список литературы

1. Энциклопедия «Касперского» // URL: https://encyclopedia-kaspersky-ru.turbopages.org/encyclopedia.kaspersky.ru/s/glossary/symmetric-encryption/ (дата обращения: 25.11.2021).

2. Youtube-видео // URL: https://www.youtube.com/watch?v=sGFbM-X6W_4 (дата обращения: 25.11.2021).

3. Youtube-видео // URL: https://www.youtube.com/watch?v=vooHjWxmcIE (дата обращения: 25.11.2021).

4. Щерба В. В. Криптографическая защита информации : курс лекций. М. : Московский университет МВД России имени В.Я Кикотя, 2016.

5. Хабр // URL: https://habr.com/ru/company/pentestit/blog/434216/ (дата обращения: 25.11.2021).

6. Криптографическая защита информации : учебное пособие / [сост. С.Г. Клюев]. Краснодар: Краснодарский университет МВД России, 2016.

7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_-LAW_112701/ (дата обращения: 25.11.2021).