УДК 316.485.6+004.7
ББК 66.4(0)+304.1
И74

ISBN 978-5-926

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
III Всероссийской научно-практической конференции

(23 апреля 2020 г.)

Краснодар
2020

Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму [Электронный ресурс] : материалы III Всерос. науч.-практ. конф., 23 апр. 2020 г. / редкол.: М. А. Ледовская, А. В. Еськов, М. Ю. Макуха, А. А. Сафронов, А. С. Арутюнов, И. Н. Старостенко, С. Ф. Самойлов, Д. Л. Куропятник, К. И. Руденко. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2020. – 1 электрон. опт. диск.

УДК 316.485.6+004.7
ББК 66.4(0)+304.1
И74

ISBN 978-5-926

И74 **Информационные и телекоммуникационные технологии** в противодействии экстремизму и терроризму [Электронный ресурс] : материалы III Всерос. науч.-практ. конф., 23 апр. 2020 г. / редкол.: М. А. Ледовская, А. В. Еськов, М. Ю. Макуха, А. А. Сафронов, А. С. Арутюнов, И. Н. Старостенко, С. Ф. Самойлов, Д. Л. Куропятник, К. И. Руденко. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2020. – 1 электрон. опт. диск.

ISBN 978-5-9266-1712-9

В сборнике представлены материалы III Всероссийской научно-практической конференции «Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму», состоявшейся в Краснодарском университете МВД России 23 апреля 2020 года.
Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму [Электронный ресурс] : материалы III Всерос. науч.-практ. конф., 23 апр. 2020 г. / редкол.: М. А. Ледовская, А. В. Еськов, М. Ю. Макуха, А. А. Сафронов, А. С. Арутюнов, И. Н. Старостенко, С. Ф. Самойлов, Д. Л. Куропятник, К. И. Руденко. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2020. – 1 электрон. опт. диск.

Содержание

ВАРИАНТЫ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ В СЕНСОРНОЙ СИСТЕМЕ МОНИТОРИНГА ПРИ ПЕРЕДАЧЕ ДАННЫХ ЧЕРЕЗ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Агибалов Никита Игоревич[1], agibalov.nikita@yandex.ru
Душкин Александр Викторович[1,2,3], a_dushkin@mail.ru

[1]Национальный исследовательский университет
«Московский институт электронной техники»
[2]Военный учебно-научный центр Военно-воздушных сил
«Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»
[3]Воронежский государственный технический университет

Аннотация. В работе проведен анализ работы сенсорной системы мониторинга сложного технологического оборудования, на основе которого сделан вывод об уровне защиты данных при ее передаче, также разработаны рекомендации для повышения защищенности данных в каналах связи.

Ключевые слова: данные, мониторинг, протокол, сенсор, система предикативной аналитики, уязвимость

В соответствии с федеральным проектом «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации» основными сквозными технологиями являются ключевые научно-технические направления, оказывающие существенное влияние на развитие новых рынков, которые не могут, в большинстве случаев, обойтись без использования сенсорных систем. Сенсорные системы предназначены для получения информации о внешней среде. В отдельных автоматизированных системах управления технологическими процессами (АСУ ТП) имеются также различные устройства – датчики, необходимые для функционирования этих систем, измерители геометрических параметров, плотности, температуры, оптических свойств, химического состава и т.д.

Рассмотрим основные принципы построения и возможности типовой перспективной АСУ ТП на примере системы предиктивной аналитики Clover SmartMaintenance на базе IIoT компании Clover Group. Данная система может быть применима для промышленных предприятий различных отраслей экономики: машиностроения, нефти, газа, металлообработки, энергетики и других отраслей российской экономики. Clover SmartMaintenance – прогнозное обслуживание и мониторинг сложного технологического оборудования на базе платформы Clover Predictive для интеллектуального анализа больших данных с применением технологий искусственных нейросетей и методов машинного обучения.

Примером применения Clover SmartMaintenance на практике может быть система интеллектуальной диагностики и прогноза технического состо-

яния «Умный локомотив», суть которого сводится к следующему. Специальные датчики и сенсоры устанавливаются на локомотиве. С них получают данные, которые поступают для интеллектуального анализа на специальную платформу во время захода локомотива локомотивное депо для проведения сервисных работ. После этого информация о состоянии поезда отправляется в главный офис, где на специальном автоматизированном месте можно увидеть отображение возможных предотказных состояний различных узлов ряда неисправностей. В ходе мониторинга выявляются скрытые неисправности подвижного состава, приводящие впоследствии к серьезным поломкам и тяжелым ремонтам. Таким образом, это приводит к экономии денег, ресурсов, усилий и времени для сервисной бригады, и, соответственно, для ОАО «РЖД». Такой способ прогнозирования неисправностей при водит к повышению эффективности работы эксплуатируемого парка локомотивов и железнодорожной инфраструктуры в целом. Так как эти данные достаточно значимы (особенно в целях предотвращения аварий и катастроф), их необходимо, соответственно, защищать.

Clover Smart Maintenance – российское программное обеспечение, выполняющие поддержку в принятии решений по проведению технических воздействий на оборудование и его узлы (техническое перевооружение и реконструкция, а также техническое обслуживание и ремонт) учетом факторов технического состояния, риска отказа и эффективности топливоиспользования с целью обеспечения требуемого уровня надежности, безопасности и эффективности на предприятии [1].

В общем плане Clover Smart Maintenance позволяет:

– в режиме реального времени на основании телеметрических данных с оборудования рассчитывать текущий и прогнозный Health Index (индекс здоровья; индекс технического состояния) и другие показатели надежности;

– выявлять перерасход условного топлива или электроэнергии на отпуск продукции вследствие некорректной работы (деградации; износа) отдельных узлов оборудования;

– выявлять неисправности в узлах оборудования и передавать их в ERP-систему для обоснованного формирования программы ремонтов или нарядов (заданий) на конкретные работы;

– производить объективную оценку качества произведенных ремонтных работ на данных телеметрии.

Решение состоит из платформы Clover Predictive и гибридных инженерно-математических МХ-моделей. Платформа имеет модульную (микросервисную) структуру и обеспечивает достаточно высокую степень адаптации применительно к специфике разнородных задач Заказчика. За счет этого достигается открытость архитектуры, и высокая гибкость с точки зрения повсеместной интеграции других программно-аппаратных комплексов Заказчика.

МХ-модели – это прогнозные модели, разрабатываемые Clover Group для обнаружения предотказных состояний и прогнозирования выхода технологического оборудования из строя, работа которого может быть в достаточ-

ной степени описана его датчиками, а также с помощью расчетных методов при построении инженерной модели [2].

Прогнозные модели, в которых инженерные исследования дополняются методами машинного обучения, анализа больших данных и нейронных сетей, дают лучший результат для оценки технического состояния сложного оборудования и высокую точность прогноза отказов.

Однако, необходимо разобраться каким образом происходит передача данных и защита информации. Протоколом передачи данных, как правило, является TCP. Данный протокол не шифрует информацию и любой злоумышленник, перехвативший данные, сможет их прочитать.

Протокол управления передачей (TCP) обеспечивает интерактивную работу между компьютерами, обеспечивает безопасность и подлинность обмена данными в сети. Также TCP необходим для обеспечения работы прикладных протоколов пользовательских приложений и протокола IP, необходимого для маршрутизации и адресации пакетов. Как правило, TCP представляет собой самостоятельный системный модуль, через который проходят вызовы функций протокола. Библиотека вызовов является интерфейсом между TCP и прикладными процессами. Соединение может быть открыто или закрыто пользователем. Также он может отправить или принять данные из установленного соединения. Любая из реализаций протокола TCP обязана обеспечивать минимум его функциональности, требуемой соответствующими стандартами. Суть работы данного протокола состоит в следующем. Для передачи данных пользовательский процесс вызывает соответствующую функцию TCP с указанием буфера передаваемых данных. Далее, согласно протоколу TCP данные упаковываются в сегменты своего стека и вызывается функция передачи протокола нижнего уровня, например, IP [3].

Большинство информационных систем подвержено различным угрозам безопасности. Для протокола TCP характерной является уязвимость, описанная в технической документации RFC 793 и RFC 1323.

В ряде случаев оно оценивается как критическое и во многом зависит от производителя системы и приложения, с которым работает. Характерным случаем применения данной уязвимости злоумышленником является ситуация, приводящая к отказу в обслуживании – так называемой DDoS атаке. При этом характер и степень опасности зависят от протокола используемого приложения. То есть при сосредоточенной бомбардировке соединения множеством TCP пакетов с набором флагов RST или SYN, содержащих IP адреса и TCP порты соответствующих источника и назначения, данное соединение может быть сброшено. Такая атака до недавнего времени считалась практически неосуществимой, так как в ходе проверки порядкового номера RST или SYN пакета получается 32-разрядное число с вероятностью правильного определения 1/232 [4-5]. При исследовании вероятности благополучного для злоумышленника исхода RST атаки получены достаточно высокие цифры, что свидетельствует о реальности осуществления такого вида нападения. Это связано с тем, что существует так называемый размер TCP окна, т.е. определенный диапазон порядковых номеров от требуемого числа.

Таким образом, для DDoS атаки уязвим любой протокол, основывающийся на долговременном TCP соединении с известными номерами TCP портов и IP адресами источника и назначения.

Для защиты от данной уязвимости целесообразно сделать следующее [4-6]: использовать протокол IPSEC, при помощи которого происходит шифрация трафика на сетевом уровне (информация TCP соединения становится недоступной), и/или размер TCP окна уменьшить до приемлемых размеров, т.к. побочным эффектом данной операции является увеличение потерь трафика и последовательной ретрансляции.

Применение протокола IPSEC повышает конфиденциальность данных и службы аутентификации на сетевом уровне. Для изменения размер TCP окна, заданного обычно по умолчанию, в Unix системах целесообразно использовать программу «sysctl», а в Microsoft Windows – с помощью модификации ключа реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ Parameters. Но при этом необходимо помнить, что изменение размера TCP окна может привести низкой производительности маршрутизирующих устройств.

Таким образом, в данной работе рассмотрена сенсорная система мониторинга сложного технологического оборудования типа «Clover» на примере системы интеллектуальной диагностики и прогноза технического состояния «Умный локомотив», ее основные задачи. Проанализирован протокол передачи данных (TCP), который используется в данной системе, и указана уязвимость, заключающаяся в возможности сброса, установленного TCP подключения, позволяющая осуществить DDos атаку. Чтобы минимизировать риск использования данной уязвимости предложено два варианта ее устранения: 1) использовать протокол IPSec, с помощью которого происходит шифрование данных; 2) уменьшить размер TCP окна. Протокол IPSEC обеспечивает конфиденциальность данных на сетевом уровне, а также поддерживает проверку подлинности конечных точек соединения и шифрование трафика между ними. Кроме того, необходимо помнить, что изменение размера TCP окна может привести низкой производительности маршрутизирующих устройств.

Литература

1. Система управления техническим обслуживанием оборудования [Электронный ресурс]. URL: https://clover.global/solutions/clover-smartmaintenance/ (дата обращения: 22.04.2020).

2. Clover group [Электронный ресурс]. URL: http://2050.digital/en/company/partners/clover-group/ (дата обращения: 20.04.2020).

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб.: Питер, 2019. 992 с.

4. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности. М.: Горячая линия – Телеком, 2016. 248 с. ISBN 978-5-9912-0470-5.

5. Долматова Я.Г., Душкин А.В., Кравченко А.С., Панычев С.Н., Сахаров С.Л. Некоторые прикладные вопросы информационной безопасности систем обработки информации. Современные наукоемкие технологии. 2016. №8-1. С. 41-45.

6. CCNA ICND2 200-101. Маршрутизация и коммутация. М.: Вильямс, 2015. 736 с.

ФОРМЫ ВЗАИМОДЕЙСТВИЯ ЭКСПЕРТНО-КРИММИНАЛИСТИЧЕСКИХ, СЛЕДСТВЕННЫХ И ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРОЯВЛЕНИЯМИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА.

Арутюнов Александр Самсонович[1], alexandr.arutyunov@gmail.com
[1]Краснодарский университет МВД России

Аннотация. В статье рассматриваются проблемные аспекты взаимодействия сотрудников правоохранительных органов при расследовании преступлений, связанных с фактами проявлений терроризма и экстремизма. Автором рассмотрены формы и внесены предложения по повышению эффективности взаимодействия сотрудников экспертно-криминалистических и следственных подразделений на различных этапах расследования преступлений данных категорий.

Ключевые слова: взаимодействие, следственно-оперативная группа, судебная экспертиза, консультация специалиста, планирование расследования.

Эффективность расследования уголовных дел, связанных с проявлениями терроризма и экстремизма зависит от взаимодействия следственных, оперативных, экспертно-криминалистических подразделений, их налаженной, четкой организации работы, как на месте происшествия, так и при любом следственном, оперативно-розыскном действии, планировании расследования, выдвижении версий по уголовному делу. Экспертно-криминалистические подразделения призваны всесторонне и оперативно обеспечивать потребности как следственных, так и оперативных подразделений в эффективном применении современных криминалистических средств и методов для предупреждения, выявления, раскрытия преступлений, связанных с терроризмом и экстремизмом, расследования уголовных дел по рассматриваемым видам преступлений. Взаимодействие рассматриваемых субъектов позволяет не только раскрыть преступление, но и в кратчайшие сроки провести необходимые исследования, судебные экспертизы, сократить срок производства по уголовному делу.

Противодействие экстремизму и терроризму – одна из главных стратегических задач национальной безопасности Российской Федерации. По решению Президента Российской Федерации в целях совершенствования государственного управления в области противодействия терроризму 15 февраля 2006 года был образован Национальный антитеррористический комитет — коллегиальный орган, координирующий и организующий антитеррористическую деятельность органов государственной власти на федеральном уровне, на уровне субъектов Российской Федерации и органов местного самоуправления [1]. В состав НАК входят руководители почти всех силовых структур, спецслужб, ключевых правительственных ведомств, а также обеих палат парламента России.

Однако, несмотря на принимаемые законодательные, организационные решения, остаются проблемы во взаимодействии при расследовании уголовных дел рассматриваемой категории, Многие ученые, а также сотрудники правоохранительных структур уже более десяти лет указывают на несовершенство взаимодействия следственных, оперативных и экспертно-криминалистических подразделений. Особенно остро стоят нерешенные проблемы при расследовании уголовных дел по преступлениям, связанным с проявлениями терроризма и экстремизма. Ситуация усугубляется высоким уровнем ксенофобии российских граждан, увеличением количества преступлений террористического характера, совершенных по экстремистским мотивам, недостатками в проведении миграционной политики, активной деятельностью зарубежных экстремистских организаций, сложностями в правоприменении уголовно-правовых норм по преступлениям, связанным с проявлениями экстремизма и терроризма, трудностями и ошибками в следственной и судебной практике расследования и рассмотрения указанной категории уголовных дел.

Изучение уголовно-правовых норм, связанных с терроризмом и экстремизмом, позволяет сделать вывод о том, что в расследовании рассматриваемых преступлений применяется широкий спектр специальных знаний, проводятся различные виды экспертиз и исследований: например, лингвистические экспертизы; психолого-почерковедческие; автороведческие; взрывотехнические; фоноскопические; баллистические; дактилоскопические, компьютерно-технические; биологические и др. Чаще всего в расследовании преступлений, связанных с экстремизмом и терроризмом исследования и экспертизы носят комплексный или комиссионный характер. Кроме того, по рассматриваемым преступлениям следователь привлекает к участию в производстве следственных действий специалиста. Для успешного расследования и раскрытия преступлений, связанных с терроризмом и экстремизмом необходимо скоординированное взаимодействие экспертно-криминалистических и следственных подразделений.

Понятие «взаимодействие» не закреплено ни в уголовно-процессуальном законе, ни в каком-либо ином федеральном законе, регламентирующем деятельность по расследованию преступлений, в том числе связанных с терроризмом и экстремизмом. Для уяснения понятия «взаимодействие» необходимо обратиться к изучению работ ученых, посвятивших свои труды вопросам взаимодействия в расследовании и раскрытии преступлений.

Так, И.А. Данилкин пишет: «взаимодействие – это согласованная, объективно обусловленная, организуемая начальниками органов и подразделений внутренних дел и направляемая следователем деятельность административно независимых друг от друга субъектов, которая выражается в наиболее эффективном сочетании присущих им методов и средств» [2, с. 48].

Т.Ф. Скогарева утверждает, что «целью взаимодействия является не только совместное проведение следственных действий, составление совмест-

ных планов, но и постоянный контакт, и взаимопомощь при проведении тех или иных мероприятий при расследовании преступлений» [3, с. 95-100].

Выражая свое согласие с И.В. Суворовой, в том, что «специфика взаимодействия следователя и эксперта при назначении и производстве экспертизы состоит в том, что такое взаимодействие хотя и предполагает их тесный контакт, но в значительной степени носит опосредованный характер и заключается в осуществлении каждым из них согласованных по целям различных взаимосвязанных действий» [4, с. 65], отметим, что взаимодействие между экспертом и следователем имеет несколько форм. Но, независимо от форм взаимодействия, эту деятельность объединяет получение тождественных знаний об обстоятельствах, подлежащих доказыванию.

В расследовании уголовных дел, связанных с проявлениями терроризма и экстремизма, принятие обоснованного решения по производству следственных действий (обыск, осмотр и др.), а также по задержанию подозреваемых лиц, зависит зачастую от выбора следователем рациональных путей выполнения задач, стоящих перед ним. Решения следователя должны быть эффективными, правильными, поскольку от них зависит раскрытие преступления, связанного с терроризмом и экстремизмом.

Т.Ф. Скогарева выделяет два критерия во взаимодействии сил и средств в процессе раскрытия и расследования преступления:

1) эффективности;

2) оптимальности [5, с. 431-434].

Первый касается результативности принимаемых решений следователем, а второй – количественный показатель эффективности, то есть выбор наилучшего варианта решения поставленной задачи.

Взаимодействие экспертно-криминалистических, следственных и оперативных подразделений при расследовании преступлений, связанных с проявлениями экстремизма и терроризма, основывается на трех условиях:

экономичность взаимодействия – означает целесообразность материальных затрат на организацию взаимодействия в расследовании, подготовку совместных мероприятий, производство следственных действий и т.п.;

безопасность взаимодействия – означает профессиональную подготовленность участников, что особенно важно в расследовании преступлений, связанных с терроризмом, при которых возможно большое количество жертв. Кроме того, безопасность при взаимодействии означает и совершенствование применения сил и средств участниками;

эффективность взаимодействия – определяется достижением поставленных целей (например, проведен осмотр места происшествия – места взрыва после террористического акта, изъяты определенные следы и т.п.).

С учетом того, что взаимодействие – это всегда коммуникативная деятельность, в юридической литературе есть несколько мнений по определению форм взаимодействия между следователем и иными подразделениями.

Среди процессуальных форм взаимодействия экспертно-криминалистических, следственных и оперативных подразделений при рас-

следовании преступлений, связанных с проявлениями экстремизма и терроризма, выделим:

совместную деятельность при производстве следственных действий, порядок которых строго регламентирован в УПК РФ;

совместную деятельность в процессе назначения, производства и оценки результата судебных экспертиз.

К непроцессуальным формам отнесем следующие:

- совместная деятельность по планированию расследования уголовных дел;

- использование экспертно-криминалистических учетов, картотек и коллекций;

- совместная работа в следственно-оперативной группе;

- консультативная или справочная деятельность экспертно-криминалистических подразделений.

Итак, формы взаимодействия экспертно-криминалистических, следственных и оперативных подразделений при расследовании преступлений, связанных с проявлениями терроризма и экстремизма, делят на процессуальные (при производстве следственных действий) и непроцессуальные (при планировании расследования, использовании экспертно-криминалистических учетов, картотек и коллекций, консультативная помощь). Вне зависимости от форм взаимодействия, у совместной деятельности указанных подразделений общие задачи коррелируют с принципами уголовного судопроизводства, основаны на принципах законности, комплексного использования сил и средств и непрерывности совместной оперативно-служебной деятельности.

Литература

1. Сайт Национального антитеррористического комитета НАК // [Электронный ресурс] URL: http://nac.gov.ru/nak/celi-i-zadachi.html. (дата обращения 12.02.2020).

2. Данилкин И.А. Взаимодействие следственных и экспертно-криминалистических подразделений органов внутренних дел. – М.: Юрлитинформ, 2010. С. 48.

3. Скогарева Т.Ф. Теоретические основы взаимодействия субъектов правоохранительных органов при расследовании преступлений // Вестник Волгоградской академии МВД России. 2014. № 2 (29). С. 94-98.

4. Суворова И.В. Взаимодействие следователя с экспертом при подготовке к назначению судебной экспертизы // Уголовное судопроизводство: проблемы теории и практики. - № 3. – 2017. – С.65.

5. Скогарева Т.Ф. Формы организации взаимодействия следственных и экспертных подразделений в ходе расследования преступлений // В сборнике: Массовые коммуникации на современном этапе развития мировой цивилизации: материалы Всероссийской научной конференции с международным участием. Гуманитарно-социальный институт. 2015. С. 431-434.

«БОЛЬШИЕ ДАННЫЕ» И БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В СОВРЕМЕННЫХ УСЛОВИЯХ

Астафьева Марина Владимировна[1], elena.u0604@mail.ru
Бегларян Маргарита Евгеньевна[1], rita_beg@mail.ru

[1]Северо-Кавказский филиал ФГБОУВО «Российского государственного университета правосудия» (г. Краснодар)

Аннотация. В данной статье исследовано новое для общества понятие «Больших данных» или «Big Data», а также его соотношение с персональными данными. Дан сравнительно-правовой анализ как существующего, так и предложенного законодательного регулирования «Big Data» в российском и международном праве. Рассмотрены возможные негативные сценарии обработки, использования и хранения этих данных. В исследовании под «Большими данными» мы будем понимать любые массивы персонализированной и не персонализированной информации, связанной с перемещением человека, количественными и качественными признаками различных видов деятельности. Эти данные получены с помощью камер видеонаблюдения, банковских транзакций, запросов в интернете, разговоров с помощью сотовой связи и много другого. Такие данные могут быть подвергнуты различным видам обработки, и полученная информация имеет огромную ценность. Она может быть интересна финансистам, экономистам, маркетологам как во благо, так и против людей.

Ключевые слова: «Большие данные», «Big Data», технология, персональные данные, безопасность, информация, обработка, использование, регулирование.

В современном мире использование новейших цифровых технологий отслеживания и накопления информации стало возможным во всех сферах жизни человека. В информационном обществе возникла необходимость контролировать и разграничивать доступ к такой информации. Сверхбольшие объемы социальной информации явились как результат развития компьютерных технологий, технологий накопления и обработки, а юридическая наука не успевает осмыслить угрозы этих явлений.

В настоящее время в условиях стремительного распространения коронавирусной инфекции, следствием чего стала необходима самоизоляция, новую актуальность приобретают технологические решения, минимизирующие прямые контакты и соприкосновения. Таким образом, возрос уровень использования дистанционных каналов существования, в рамках которых необходимо «подтверждать себя», что обычно происходит посредством использования персональных данных с последующей обработкой .

Государства прибегли к использованию систем отслеживания, которые формируют «Большие данные». Например, противостоять пандемии возможно с помощью технологии «Большие данные» для отслеживания и прогнозирование.

Без технологий отслеживания не обходится и Россия. Осуществляется отслеживание лиц, которые могли контактировать с зараженными, то есть потенциально инфицированных. В их число попадают как люди из ближнего круга заболевших, так и во многом пассажиры некоторых рейсов, курьеры, водители такси и т.д. Оповещают всех, контактировавших с заболевшим, о необходимой самоизоляции посредством SMS-рассылки. Таким образом удалось найти около тысячи человек, которые имели риск заражения [1].

Используются при этом, так называемые, «Большие данные», которые не являются персональными. Но насколько соблюдается эта грань между «Большими данными» и персональными данными и кем осуществляется сбор и хранение этих больших объемов данных?! Не приведет ли использование данных технологий к «тотальной слежке» со стороны заинтересованных организаций?!

В настоящий момент в регулировании использования «Больших данных» системообразующими актами являются ФЗ № 152-ФЗ «О персональных данных» [2] (Далее - ФЗ о Персональных данных) и ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3].

Российское законодательство на данный момент не оперирует понятием «Большие данные», регулируя их как персональные данные. Однако вопрос закрепления законодательного регулирования этих данных обсуждался не раз.

Европейский законодатель[4] расширил понятие «персональных данных», включив в него понятие «Больших данных». В российском же законодательстве отмечается неопределенность: предлагаемые законопроекты указывают, что «Big Data» не должны содержать персональные данные, хотя последние определяются как любая косвенная информация, относящаяся к определенному физическому лицу (ст. 3 ФЗ о Персональных данных). Принятый 6 июля 2016 г. Пакет Яровой[5,6] обязывает операторов связи и организаторов распространения информации хранить не только персональные данные, но и метаданные, передаваемые пользователями. Таким образом, Пакет Яровой в большой мере распространяется на «Большие данные», ФЗ о Персональных данных – лишь отчасти[7]. К тому же Пакет Яровой, по сути, является первым документом, который на законодательном уровне заявил о публичном сборе, хранении и использовании этих данных в целях борьбы с терроризмом.

23 октября 2018 года в Государственную думу РФ был внесен законопроект[8], который предусматривал регулирование обработки «Больших пользовательских данных». В соответствии с п. 2 ст. 1 Законопроекта под «Большими пользовательскими данными» предлагалось понимать «совокупность не содержащей персональных данных информации о физических лицах и (или) их поведении, не позволяющая без использования дополнительной информации и (или) дополнительной обработки определить конкретное физическое лицо, собираемой из различных источников, в том числе сети «Интернет», количество которой превышает тысячу сетевых адресов».

Анализируя предлагаемое в Законопроекте регулирование обработки «Больших пользовательских данных», которое во многом копирует положения ФЗ о персональных данных, можно сделать вывод, что оно поверхностно затрагивает проблемы, которые касаются обработки «Big Data», т.е. не содержит должного регулирования.

К тому же не вполне понятно, как предложенное регулирование будет соотносится с ФЗ о персональных данных. Поскольку большинство компаний, которые осуществляют обработку «Больших данных» (мобильные операторы, банки), владеют и персональными данными пользователей, законопроект или в принципе не будет применяться, так как данные в совокупности будут связаны друг с другом и являться персональными данными, или в случае, если данные будут разделены, то возникнет необходимость в двойном регулировании (получать от субъектов данных два согласия, вести два реестра и т. п.).

Следует также отметить, что указанное определение «Больших данных» привязывает их к конкретному сетевому адресу. Однако сетевой адрес может позволить идентифицировать соответствующего пользователя. В этом случае данные будут являться именно персональными данными, так как косвенно позволяют идентифицировать физическое лицо.

Примечательно, что в европейский законодатель относит сетевой адрес к персональным данным: Общий регламент ЕС по защите данных (GDPR) предусматривает, что IP-адреса, как и иная метаинформация, могут быть отнесены к персональным данным (п. 30 Преамбулы).

Интересным становится порядок получения информированного согласия на обработку «Больших пользовательских данных». Так как для его дачи пользователь должен идентифицировать себя, либо будет невозможно установить, что конкретный пользователь дал свое согласие. Однако, в случае идентификации субъекта, его данные автоматически становятся персональными данными.

Таким образом, не до конца ясно, что такое информация, которая не содержит персональных данных, но относится к физическим лицам и их поведению. Под данные критерии подходят статистические данные, но вряд ли «Big Data» ограничивается статистикой.

Несомненно, регулирование использования «Big Data» необходимо, но все-таки, так как предлагаемое регулирование ставит под угрозу безопасность персональных данных, реализация такого регулирования должна быть осуществлена с привлечением соответствующих специалистов, для которых, в принципе, понятие «Больших данных» не является новым, оно существует давно, но только сейчас вышло на арену закона.

В феврале 2020 года Минкомсвязь разработала и предложила законопроект, который направлен на регулирование рынка «Больших данных». В документе вводятся определения понятий «Большие данные», «оператор Больших данных» и «обработка Больших данных». Предполагается, что Роскомнадзор будет контролировать оборот «Big Data». Для этого будет со-

здан реестр операторов «Больших данных». Однако данный проект также называют сырым и непродуманным[9].

Предложенное в законопроекте определение «Больших данные» значительно отличается от вышеуказанного, перечисляются непосредственно сведения, которые относятся к «Большим данным» (информационные и статистические сообщения, сведения о местоположении движимых и недвижимых объектов, количественные и качественные характеристики видов деятельности, поведенческие аспекты движимых и недвижимых объектов). Однако, мы считаем, что «Большие данные», в принципе, невозможно определить как объект, поскольку это динамичный, безостановочный процесс появления новых данных, часть которых изначально не структурирована и не обработана, а часть уже выступала предметом обработки. Отличительные особенности «Больших данных», скорее, относятся к алгоритму обработки и использования. В этой связи интересным становится вопрос определения порядка доступа к регулируемым данным, где будет храниться такой объем информации и в каких целях данная информация может быть использована.

Итак, очевидно, что «Большие данные» являются признаком современного общества, явлением, которое имеет характеристики объекта, по нашему мнению, следует законодательно закрепить четкое разграничение между «Большими данными» и персональными данными.

Решение данной проблемы мы видим в разработке и принятии отдельного законодательного акта, который может содержать следующие положения о «Больших данных»:

- обезличенность, насколько это возможно;
- прямая или косвенная информация, относящаяся к человеку;
- придание им некоторых свойств персональных данных: конфиденциальность, непередача третьим лицам, особый статус оператора «Больших данных», ограничение этих операторов по использованию персональных данных;
- необходимость создания такого алгоритма, который будет регулировать безопасную обработку, использование, хранение, а также их уничтожение.

Стоит отметить, что использование «Больших данных» во всем мире в частности сейчас выгодно и государству, и организациям в маркетинговой сфере, так как цифровые технологии, мобильные устройства и социальные сети стали неотъемлемой частью повседневной жизни людей во всем мире. Так, количество интернет-пользователей в мире достигло 4,54 миллиарда. В России, по данным Digital 2020, 118 миллионов интернет-пользователей. Это значит, что интернетом пользуются 81% россиян. Среднестатистический пользователь проводит в интернете 6 часов 43 минуты каждый день[10].

Таким образом, главной проблемой в отношении повсеместного распространения «Big Data» и невозможности решения современных задач (угроза COVID-19) является вопрос безопасности хранения этих данных. Так как происходит глобальное сосредоточение различной информации, необходимо приложить максимум усилий для защиты таких данных. Баланс между

будущим и настоящим с применением «Больших данных» возможен только в том случае, если будут использованы все преимущества современных технологий, привлечены IT-специалисты и применено интегративное правовое регулирование.

Литература

Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. // Собрание законодательства РФ. 2014. № 9. Ст.851;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3451;

Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448;

https://eugdpr.org [электронный ресурс], Общий регламент ЕС по защите данных (GDPR) // (дата обращения: 01.04.2020);

Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»//Собрание законодательства РФ. 2016. № 28. Ст. 4558;

Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»// Собрание законодательства Р. 2016. № 28. Ст. 4559;

7. Соснин К.А. Правовое регулирование Больших данных: зарубежный и отечественный опыт//Журнал Суда по интеллектуальным правам. № 25. 2019 г. С. 30-42;

8. http://sozd.parliament.gov.ru/bill/571124-7 [электронный ресурс], Законопроект // (дата обращения: 01.04.2020);

9. https://www.comnews.ru/content/204636/2020-02-18/2020w08/minkoms vyaz- predlozhila-regulirovat-big-data [электронный ресурс], Минкомсвязь предложила регулировать big data // (дата обращения: 01.04.2020);

10. https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ [электронный ресурс], Вся статистика интернета на 2020 год — цифры и тренды в мире и в России // (дата обращения: 08.04.2020).

НЕКОТОРЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ХОДЕ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ

Афанасьев Евгений Владимирович[1], evgenyafanasjev@yandex.ru

[1]Краснодарский университет МВД России

Аннотация. В статье рассматриваются перспективные возможности использования современных технических средств и методов при проведении осмотра места происшествия.

Ключевые слова: место происшествия, осмотр, современные технологии, беспилотные летательные аппараты, дроны, квадракоптеры, мультикоптеры.

Осмотр места происшествия является первоначальным и неотложным следственным действием и заключается в процессе собирания информации о преступном событии, которое произошло на месте его совершения. Это является одним из самых сложных способов извлечения информации. характеризующей личность преступника. Необходимо отметить, что психологический анализ места преступления (осмотр места преступления) часто является решающим, и особенно в случаях расследования преступлений с тяжкими последствиями и особенностью осмотра, который характеризуется большой степенью неопределенности.

В связи с этим крайне важно быстро и качественно обнаружить, зафиксировать, изъять и задокументировать всю информацию, обнаруженную на месте совершения преступного деяния (материальные и идеальные следы преступления), которая может помочь в короткие сроки раскрыть и расследовать преступление и, в конечном счете, привлечь к ответственности тех, кто нарушил закон.

При грамотном подходе к проведению осмотра у следователя и других лиц, принимающих активное участие в осмотре места совершения противоправного деяния, появляется реальная возможность получения ценной криминалистически значимой информации, способной повысить успешность раскрытия и расследования преступления. Такой осмотр позволяет получить данные, которые дают возможность охарактеризовать все стороны происшествия.

Следует отметить, что, рассматривая осмотр места преступления как первоначальное (неотложное) следственное действие, он выступает как наиболее близкий во времени и пространстве контакт следователя с событием преступления и его последствиями. Неотложное - потому, что следы, считаясь истинными «свидетелями» преступления могут быть утрачены или быть искажены в результате природно-климатических особенностей, а также чрезмерной любопытности граждан, что существенно затрудняет процесс своевременного и качественного расследования преступления.

Вместе с тем, осмотр места происшествия является одним из самых сложных следственных действий и требует серьезной организации. В каждом конкретном случае необходимо определить состав участников осмотра места происшествия, необходимые технические средства для его производства и т.д. Как замечает, В. А. Воткин, именно применение современных технических средств обнаружения и фиксации следов преступления, а также обстановки места происшествия в целом повышает качество этого следственного действия [2, с. 11]. Так, например, использование компьютерной сферической фотопанорамы (КСФП) существенно увеличивает информативность результата фотосъемки, поскольку методом КСФП происходит охват места происшествия на 360º. Данный метод применения КСФП предоставляет следующие возможности, по сравнению с обычной фотосъемкой:

1) в необходимое место панорамы возможно включение любой фотосъемки: ориентирующей, обзорной, узловой, детальной;

2) появляется возможность просмотра места происшествия не только с центральной точки фотосъемки, но и с различных сторон из других необходимых точек осмотра, например, при перемещении из одного помещения в другое;

3) возможность «всплытия» на экране при наведении курсором на значок следа не только в виде фотоизображения, но и в виде текста;

4) возможность комбинирования фиксации хода осмотра места происшествия разными техническими средствами;

5) возможность «привязки» поясняющего элемента плана или схемы к конкретной точке осмотра.

Необходимо обратить внимание на тот факт, что развитие научно – технического прогресса в настоящее время дает возможность осуществлять фото и видеозапись даже в тех местах, в которые затруднительно попасть следователю для фиксации обстановки. С этой целью применяются беспилотные летательные аппараты: дроны, квадракоптеры, мультикоптеры.

Данные технические средства могут успешно применяться как в деятельности по раскрытию преступлений, то есть, при производстве оперативно – розыскных мероприятий, так и в уголовно – процессуальной деятельности при производстве отдельных следственных действий.

Если рассматривать возможности применения таких технических средств в ходе оперативно – розыскной деятельности, то здесь эффективным является использование беспилотных летательных аппаратов в производстве таких оперативно – розыскных мероприятий, как наблюдение и обследование помещений, зданий, сооружений, участков местности и транспортных средств [5, с. 82].

Преимуществами применения рассматриваемых средств фиксации в ходе оперативно – розыскного мероприятия «наблюдение» являются следующие:

возможно его применение незаметно для объекта оперативно – розыскного мероприятия, на значительном расстоянии от лица, производящего данное оперативно – розыскное мероприятие;

скорость передвижения беспилотных летательных аппаратов позволяет отслеживать объект в движении, даже на транспортном средстве;

трансляция изображения при осуществлении с помощью беспилотного летательного средства видеозаписи в режиме реального времени позволяет, при необходимости, своевременно принять решение о задержании (например, в момент передачи оружия сбытчиком покупателю; изъятия наркотического средства из места закладки) [7, с. 174].

При использовании беспилотного летательного средства в ходе оперативно – розыскного мероприятия «обследование» различных объектов, преимущества фактически те же, но дополнительным плюсом является возможность фиксации обстановки на объекте без проникновения в него человека, что особенно ценно при отсутствии уверенности в безопасности данного объекта.

Если вести речь о применении беспилотных летательных аппаратов при производстве следственных действий, то наиболее целесообразно использовать его в ходе осмотра места происшествия по различным видам преступлений, в особенности, на участках местности обширной площади, границы осмотра которой определены следователем или ограничены высотой и дальностью полета используемого беспилотника, а также в труднодоступной местности. К последней можно отнести болотистые местности, высокогорные участки, лесные заросли, а также сложные участки дорог [1, с. 165].

В крупных городах такие средства фиксации целесообразно использовать при проведении осмотров мест происшествий по делам о дорожно-транспортных происшествиях на сложных участках дорог, в сложных погодных условиях, при большом скоплении пострадавших машин.

Многоуровневые развязки крупных автодорог можно в полной мере назвать труднодоступным участком по следующим причинам:

ограничение проезда по одной из полос движения для проведения ремонтных работ уже вызывает трудность для продвижения по такому участку дороги; ограничение одной полосы для производства ОМП на таком участке дороги создаст трудности не только для участников движения, но и для участников осмотра, одновременно создавая опасность для личной безопасности сотрудников органов внутренних дел, участвующих в осмотре места происшествия;

перекрытие всего участка дороги для проведения осмотра невозможно, так как создаст условия невозможности движения в конкретном направлении, особенно в случае если участок осмотра места происшествия является участком для совершения маневра автотранспортом;

– большое скопление пострадавших в дорожно-транспортных происшествиях на таких сложных участках дороги автомобилей и в случаях, когда количество автомобилей превышает 5 штук, осложняет работу специалиста – криминалиста на месте происшествия, особенно в том случае, когда взаимное расположение столкнувшихся автомобилей кучное, а не линейное;

– проведение осмотра места происшествия в сложных погодных условиях (туман, снегопад и т.д.), также вызывает сложности, связанные с производством фото- и видеосъемки для фиксации общей обстановки места происшествия, положения автомобилей, удаленно расположенных от места фотографирования (в случае наличия дорожных ограждений, играющих очень важную роль при ДТП, предотвращая вылет автомобиля с дороги на обочину, а также с мостов и мостовых сооружений), детальной фиксации повреждений при кучном скоплении автомобилей [4].

При всех вышеперечисленных объективных условиях использование беспилотного летательного средства, оснащенного фото-, видеоаппаратурой способствует успешному проведению осмотра места происшествия и достоверной фиксации деталей столкновения, в то время как общепринятые приемы съемки недостаточно отражают обстановку мест происшествий, имеющих значительные размеры площади.

Ввиду специфики таких мест происшествий, применение беспилотных летательных аппаратов для аэрофото - / видеосъемки деталей происшествия может быть не только дополнительным к традиционным технико-криминалистическим средством фиксации места происшествия, но и единственно возможным самостоятельным средством в конкретной оперативной ситуации, способным выполнять традиционные виды фотосъемки, применяемые при осмотре места происшествия:

ориентирующую - для фиксации общего вида места происшествия с привязкой к окружающей территории;

обзорную - для фиксации непосредственно самого места происшествия;

узловую - для фиксации крупным планом места соприкосновения столкнувшихся машин в момент удара;

детальную – для фиксации непосредственно самих следов столкновения.

Аналогичным образом может быть полезно применение беспилотных летательных аппаратов при раскрытии и расследовании незаконных рубок. Помимо того, что в ходе осмотра места происшествия с воздуха можно определить границы места происшествия, также возможно и выявление дополнительных мест совершения незаконных рубок, о которых правоохранительным органам ранее было неизвестно [6, с. 271]. Также, с помощью беспилотных летательных аппаратов можно зафиксировать и сам момент осуществления незаконной рубки, что, впоследствии, может выступить ценным доказательством.

Еще одно очень важное качество рассматриваемых технических средств фиксации – возможность его применения там, где находиться человеку опасно. Это, в частности, может касаться необходимости произвести осмотр места пожара, когда существует угроза сильного задымления, обрушения здания и т.д.

Таким образом, разумно используя возможности беспилотных летательных аппаратов, в ходе осмотре места происшествия возможно в кратчайшие сроки произвести качественную фото- и/или видеосъемку на любой местности, независимо от ее масштабов, рельефа и растительного покрытия, а также труднодоступности объекта, подлежащего фото-, видеосъемке, затрачивая минимум усилий благодаря тому, что они могут управляться как в автоматическом, так и в ручном дистанционном режиме. Так же роботизированные комплексы, установленные на беспилотных летательных аппаратах, могут обеспечить поиск, обнаружение и отождествление объектов в режиме реального времени.

Подводя итог, можно отметить, что основное преимущество использования беспилотных летательных аппаратов с функцией фото и видеозаписи в оперативно – розыскной и уголовно – процессуальной деятельности заключается в возможности фиксации местности с высоты, на удалении от наблюдаемого объекта, возможности зависания над определенным местом, детальной передачи изображение, передачи изображения в режиме реального времени, обеспечения безопасности сотрудников, производящих оперативно – розыскные мероприятия и следственные действия. Но здесь следует учиты-

вать и определенные недостатки: отсутствие данного устройства в большинстве территориальных органов, отсутствие специалистов, умеющих обращаться с ним, возможность использования только на открытых участках местности, достаточно непродолжительное время, невозможность признания доказательством полученного изображения или записи в случае нечеткости, обусловленной значительным расстоянием от точки съемки до объекта.

Таким образом, можно сказать, что далеко не все доступные следователю научно-технические средства применяются в практической деятельности в борьбе с преступлениями [8]. Недостаточность их применение как считает А.А. Давыдов, обусловлена в первую очередь с тем, что российские правоохранительные органы (особенно в регионах) пока не достаточно оснащены техническими средствами, а также в связи с тем, что существенная часть следственных работников не имеет достаточных умений и навыков по их применению [3, с. 130].

Также можно отметить не достаточное участие специалистов в расследования, прежде всего осмотре места происшествия по различным причинам. Данная причина крайне важна, так как ни дознаватель, ни следователь не в состоянии владеть технико-криминалистическими средствами и методами так же профессионально, как ими владеют сотрудники экспертно-криминалистических подразделений, которые имеют глубокую специальную подготовку, ежедневную практику, опыт применения, а также регулярно повышают свою квалификацию.

Литература

1. Бегалиев Е.Н. О перспективах применения беспилотных летательных аппаратов в ходе производства отдельных следственных действий // Вестник Восточно – Сибирского института МВД России. 2019. № 2 (89). С. 163-173.

2. Воткин В.А. О некоторых особенностях тактики осмотра на первоначальном этапе расследования разбойных нападений в СКФО // Российский следователь. 2017. N 23. С. 11-13.

3. Давыдов А. А. Проблемы использования научно-технических средств при расследовании преступлений в сфере экономики в Российской Федерации // Молодой ученый. 2018. № 44. С. 130-133.

4. Дубовик Е.С., Соколова А.Ю. Возможности использования беспилотных летательных аппаратов при проведении осмотра места происшествия по делам о ДТП // Актуальные вопросы юридических наук в современных условиях. Сборник научных трудов по итогам международной научно-практической конференции. Санкт-Петербург, 2017. № 4.

5. Осипенко А.Л. Перспективы использования информационно – аналитических технологий в оперативно – розыскной деятельности // Общество и право. 2018. № 4 (66). С. 80-87.

6. Рывкин С.Ю. Инновационные аспекты и тенденции тактики производства осмотров с использованием беспилотных авиационных средств // Современный ученый. 2019. № 6. С. 269-279.

7. Рывкин С.Ю. Малые беспилотные авиационные системы как инновационные элементы технико – криминалистических средств // Право и практика. 2019. № 4. С. 173-177.

Афанасьев Е. В. Особенности привлечения экспертно-криминалистических подразделений при расследовании незаконного оборота специальных технических средств, предназначенных для негласного получения информации // В сборнике: Криминалистика и судебно-экспертная деятельность: теория и практика материалы VI Международной научно-практической конференции. Краснодарский университет МВД России. 2018. С. 21-25.

МЕТОДИКА ИСПОЛЬЗОВАНИЯ ПРОГРАММНЫХ ЛОВУШЕК В WEB-ПРИЛОЖЕНИЯХ ДЛЯ СБОРА ИНФОРМАЦИИ О ЛИЦАХ, ПРОЯВЛЯЮЩИХ ИНТЕРЕС К ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Богданов Дмитрий Сергеевич[1], bdkrdu@yandex.ru
Горюн Кристина Николаевна[1], kngoryun@yandex.ru

[1]Краснодарский университет МВД России

Аннотация. Выявлены проблемы в области раскрытия и расследования преступлений в сфере компьютерной информации, рассмотрена методика идентификации лиц, проявляющих интерес к экстремистской и террористической деятельности в сети Интернет, посредством использования Web-ловушки (honeypot).

Ключевые слова: методика, экстремизм, терроризм, Web-приложение, honeypot, Web-ловушка.

Учитывая современные тенденции роста популярности сети Интернет стоит отметить, что такого рода популяризация несет в себе различного рода угрозы, которые могут возникнуть в условиях современного общества. Одной из таких угроз является вовлечение граждан в деятельность экстремистских и террористических организаций и группировок. На сегодняшний день одним из самых эффективных средств пропаганды сведений любого рода является глобальная сеть Интернет в которой сосредоточен огромный потенциал, одним из направлений которого является возможность доведения информации до неопределенного круга лиц в минимально короткие сроки. В рамках данной статьи сеть Интернет будет рассматриваться как инструмент пропаганды экстремизма и терроризма, а также как средство вовлечения граждан в деятельность экстремистских и террористических организаций.

Актуальность исследования сети Интернет как средства вовлечения граждан в экстремистскую и террористическую деятельность обусловлена рядом факторов, ключевым из которых является рост числа преступлений экстремисткой направленности, которые были совершены средствами информационно-телекоммуникационных технологий [1]. Также стоит отметить, что за последние три года число уголовных дел об экстремизме в сети Интернет возросло в пять раз [2].

Как известно, процесс раскрытия и расследования преступлений в сфере компьютерной информации, имеет достаточно широкий спектр проблемных вопросов, одним из которых выступает проблема идентификации лиц, совершивших то или иное правонарушение.

Одним из возможных способов получения информации о лицах, заинтересованных в экстремисткой и террористической деятельности, может быть использование программных ловушек (Honeypot) в Web-приложениях. Honeypot – в данном контексте представляет собой Интернет-ресурс приман-

ку, который будет использован правоохранительными органами для сбора информации о лицах, получающих доступ к этому ресурсу [3].

Возможность получения информации о лицах, посетивших такой ресурс возможна благодаря функциям серверных языков программирования, в данном случае будет рассмотрен язык программирования PHP, на основе которого функционирует более 80% современных Web-сайтов [4]. Средствами данного языка программирования можно получить следующую информацию о клиенте, посетившем Интернет-ресурс, заранее подготовленный сотрудниками правоохранительных органов:

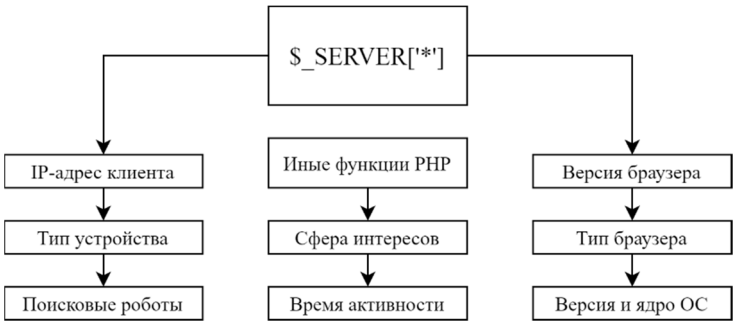


Рисунок 1. Возможности серверного языка программирования PHP в контексте сбора информации о клиенте

Как видно из Рисунка 1 серверный язык программирования PHP предусматривает достаточно большое количество функций для сбора информации о клиенте. Основополагающим средством получения такого рода информации является массив $_SERVER[*], который осуществляет обработку и хранение описанной выше информации, в зависимости от параметра, который будет передан в этот массив – он вернет соответствующий перечень сведений, необходимый администратору ресурса.

Основная идея рассматриваемой методики заключается в разработке фальшивого Web-ресурса, который будет содержать ложные сведения экстремистской и террористической направленности и в перспективе может привлечь внимание заинтересованных данной тематикой лиц. Наполнение ресурса контентом должен осуществлять сотрудник, обладающий актуальными познаниями в области террористической и экстремистской деятельности. Техническая реализация такого способа получения информации может быть выполнена техническим специалистом соответствующего подразделения органа внутренних дел.

После технической реализации и наполнения Web-ресурса соответствующим контентом следует разместить ресурс в сети Интернет. Корректное размещение ресурса напрямую влияет на эффективность способа получения информации. Ресурс может быть размещен как в открытом Интернете, так и в глубинном Даркнете. Для достижения наибольшего эффекта следует проиндексировать ресурс в поисковых системах Яндекс и Google, что даст возможность заинтересованным лицам получать к нему доступ посредством

использования поисковых систем, так как такой способ получения информации из открытого Интернета будет использован злоумышленниками в первую очередь.

При подключении заинтересованно лица к Web-ловушке, при условии соответствующей реализации, о нем будут получены сведения, указанные на Рисунке 1, которые могут быть использованы в процессе раскрытия и расследования преступлений экстремистской и террористической направленности. Процесс формирования базы данных, содержащей информацию о заинтересованных лицах, получавших доступ к ресурсу, может быть реализован средствами языка программирования PHP и MySQL в стеке с веб-интерфейсом phpMyAdmin, предназначенным для организации хранения данных на сервере.

Общая структура требований к созданию подобного ресурса представлена на Рисунке 2.

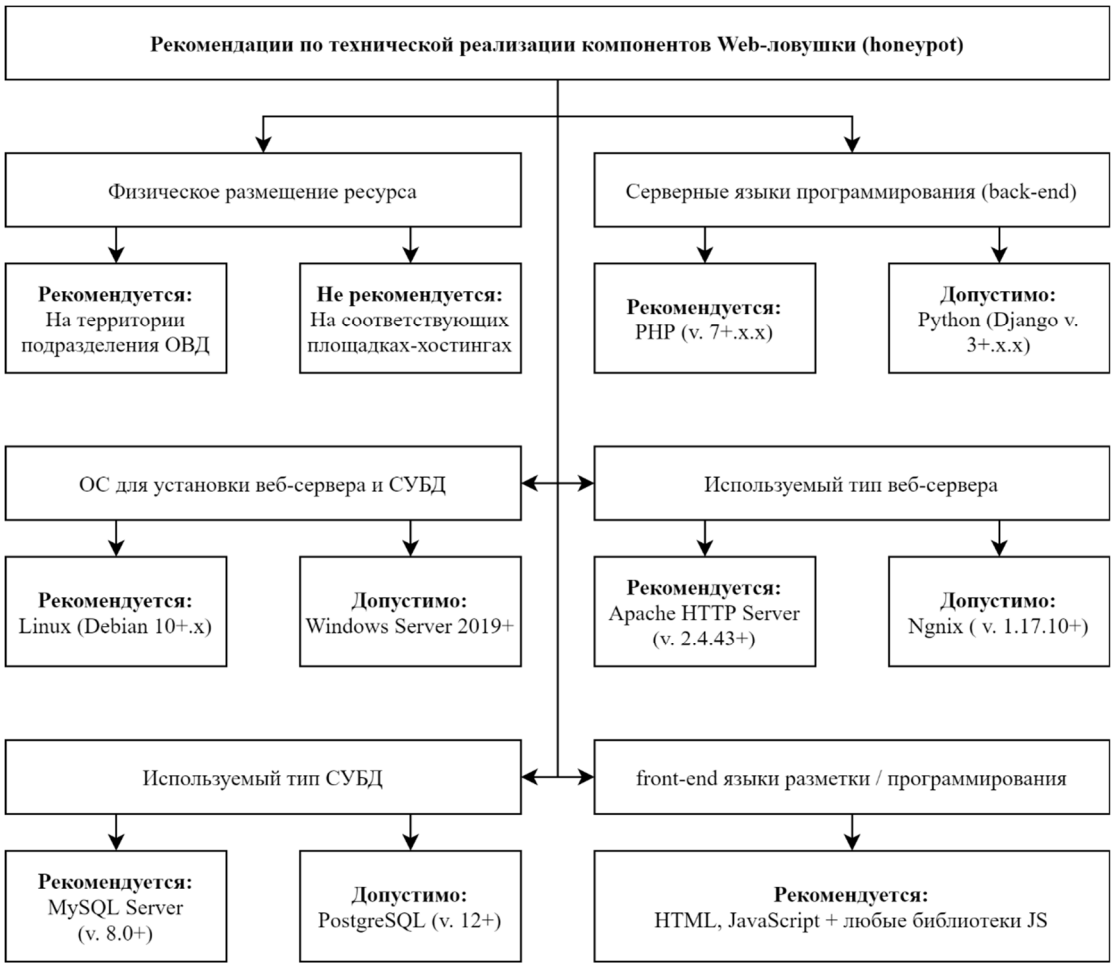


Рисунок 2. Рекомендации по технической реализации компонентов Web-ловушки (honeypot).

Современные способы совершения преступлений требует современных решений, направленных на противодействия указанным правонарушениям. При условии правильного выполнения вышеуказанных рекомендаций со-

трудники органов внутренних дел соответствующих подразделений сумеют получить информацию о лицах, которые потенциально могут иметь отношение к экстремистской и террористической деятельности, что может способствовать своевременному получению оперативно значимой информации, которая может быть использована для раскрытия и расследования преступлений в рассматриваемой области. Достоинством данного способа в первую очередь являются: простота реализации, минимальные временные затраты на техническое обслуживание (для достижения высоких показателей эффективности требуется постоянная актуализация контента) и низкие требования к аппаратному обеспечению ресурса.

Литература

1. Гаврилин Ю.В., Шмонин А.В. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности // Труды Академии Управления МВД России. 2019. № 1 (49). С. 105–111.

2. Тронева В.Н. Проблема распространения экстремизма в Интернет-среде // Научный Вестник Волгоградского Филиала Ранхигс. Серия: Юриспруденция. 2019. Т. 5. № 2. С. 85–89.

3. Sekar K.R. и др. Dynamic Honeypot Configuration for Intrusion Detection. : Institute of Electrical and Electronics Engineers Inc., 2018. С. 1397–1401.

4. 80% of the web powered by PHP [Электронный ресурс]. URL: https://haydenjames.io/80-percent-web-powered-by-php (дата обращения: 26.04.2020).

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ РАБОТЫ С ДОКАЗАТЕЛЬСТВАМИ, ПОЛУЧЕННЫМИ ПОСРЕДСТВОМ ЦИФРОВЫХ СПОСОБОВ ФИКСАЦИИ ИНФОРМАЦИИ

Газизов Вячеслав Абдуллович[1], vagaz48@rambler.ru
Подволоцкий Игорь Николаевич[2], inpodvolockij@msal.ru

[1]Московский университета МВД России имени В. Я. Кикотя
[2]«Московский государственный юридический университета имени О.Е. Кутафина (МГЮА)»

Аннотация. В статье авторы обращают внимание на проблемы формирования процессуальных доказательств в эпоху цифровизации криминалистики и судебной экспертизы. В частности, речь пойдет о развитии механизмов обеспечения предсказуемости процедур обработки электронных документов и достоверности получаемых результатов.

Ключевые слова: цифровая криминалистика, электронный документ, достоверность фото- и видео доказательств,

Введение электронных документов в процессуальную сферу породило необходимость введения дополнительных механизмов обеспечения достоверности цифровых доказательств.

Научно-технические предпосылки трансформации криминалистики и судебной экспертизы тесно связаны с цифровым веком, цифровым пространством, цифровыми технологиями.

Процессуальным наукам еще предстоит определиться с терминологией и разработать методические рекомендации, соответствующие принципам создания электронных документов, и цифровым способам фиксации доказательственной информации [1]. В этой связи возникают вопросы, имеющие отношение к свойствам подобных следов и насколько они отвечают требованиям уголовного процесса, криминалистики и судебной экспертизы, как доказательств в сфере судопроизводства.

В настоящее время цифровые устройства используются для фиксации результатов следственных действий и судебных экспертиз, однако их технические параметры и программное обеспечение соответствуют только требованиям коммерческого сектора, что явно недостаточно для фиксации судебных доказательств и процедур. Основным недостатком мобильных фотографических средств является низкая степень обеспечения достоверности фото-, видеоизображений, приобщаемых к материалам судебного дела.

Возможности цифровой обработки изображений заложены в базовые функции современных фото-, видеоустройств, что позволяет в автоматическом режиме получать насыщенные и детальные фотокадры. Производители, из коммерческих соображений, не раскрывают алгоритмы обработки промежуточных образов. Можно только предполагать за счет чего происходят эти изменения. Наиболее простой способ улучшения контрастности изображений заключается в исключении слабо-видимых деталей и усилении имеющихся, при этом получаемый фотоснимок места происшествия может утратить часть визуальной информации. С видеоизображениями все гораздо сложнее, поскольку для сокращения объема конечной видеозаписи происходит деление всей видеограммы на опорные и второстепенные кадры, при этом последние содержат только часть запечатленного события. В подобной ситуации следует задуматься насчет достоверности доказательств, фиксируемых с помощь мобильных смартфонов.

На сегодняшний день смартфоны, прежде чем попасть в руки потребителю проходят обязательную сертификацию на безопасность для пользователя, на соответствие правилам и нормам технического регламента Таможенного союза. Устройства не должны оказывать дестабилизирующего воздействия на целостность, устойчивость функционирования и безопасность единой сети электросвязи Российской Федерации. Но на достоверность и адекватность фото- видео фиксации объектов и воспроизведения полученных изображений с помощью таких устройств, проверка не проводится.

Достоверность полученных изображений, для фиксации информации криминалистически значимых объектов, при использовании фото- видео технических средств (фото-видеокамер, камер видеонаблюдения, смартфонов и

т.п.) необходимо подтверждать сертификатом соответствия. Применение в правоохранительной деятельности несертифицированных, нелицензионных технических средств и программного обеспечения может привести к экспертным ошибкам, в конечном счете, порождает недостоверную доказательственную информацию. Р.С. Белкин еще в начале 2000 годов указывал на причины экспертных ошибок, среди которых отмечал неадекватные математические модели и компьютерные программы[2].

Представляется, что дальнейшее использование цифровых фоторегистрирующих устройств общего назначения (для фотолюбителей, пользователей мобильных устройств и т.п.) в правоприменительной деятельности будет подвергнуто серьёзному правовому и организационному анализу. По нашему убеждению, обязательность применения сертифицированных фоторегистрирующих устройств и их программного обеспечения для целей использования в биометрических системах и судопроизводстве должна быть закреплена федеральным законом. Эта мера связана с необходимостью исключить случайное или умышленное вмешательство в процесс фото- и видеофиксации доказательств.

Изложенное позволяет говорить о необходимости создания «цифрового негатива», защищенного криптографическими технологиями. Полученное, сертифицированным техническим средством достоверное цифровое изображение криминалистически значимого объекта может демонстрироваться доступными способами визуализации при предъявлении доказательств во время следственного или судебного разбирательства, без вмешательства в первоначальное содержание.

Известно, что фото-, видеоизображение может быть самостоятельным объектом экспертного исследования, к примеру, фототехнической или портретной экспертизы. Цифровая обработка изображений — это область знаний, которая использует различные методы и находит применение в правоохранительной деятельности[3]. В этой ситуации эксперту представляется «код доступа», что позволит произвести необходимые для исследования манипуляции (кадрирование, улучшение различимости индивидуальных признаков объектов или применение фотографических методов сопоставления).

Уже в конце прошлого века эксперты задавались вопросом о безопасности использования цифровых технологий в правоохранительной деятельности и достоверности отображения запечатлённых характеристик объектов и явлений. На сегодняшний день мы осознаем в полной мере то, что действующая система работы с цифровыми доказательствами, защищается только «честным словом» оператора фото -, видеокамеры и угрозой наказания за фальсификацию доказательств. Думается, что этого недостаточно.

При близком рассмотрении вопроса, видится три проблемы, которые обозначились наиболее остро. Первая связана с необходимостью использования специализированного программного обеспечения для цифровой обработки изображений в сфере правоохранительной деятельности, гарантирующего достоверное, адекватное изображение, полученное в результате применения допустимых методов. Вторая проблема – отсутствие полноценной норматив-

ной базы, ограничивающей использование бытовых фото -, видеоустройств в сфере государственных интересов. Третья проблема – низкая квалификация персонала, применяющего цифровое оборудование.

Возникновение первой проблемы обусловлено тем, что при производстве экспертизы необходимо использовать специальное программное обеспечение, позволяющее эксперту выявлять условия фотографирования и технические параметры примененного для записи оборудования. Осуществлять подготовку объектов для исследования и эффективно применять методы сравнения, а также наглядно оформлять результаты исследования. Каждый этап проведения портретного исследования требует отражения в текстовой части заключения. Эксперту необходимо указать массу сведений в отношении содержания и результатов примененных методик, а также последовательность программных манипуляций с объектами экспертизы. Методы и приемы, которые применяет эксперт при проведении исследования с использованием компьютерных программ, достаточно сложные и громоздкие. В некоторых случаях, чтобы получить результат, требуется использование нескольких разнообразных программ. Например, при производстве портретного исследования по видеоизображению, где одна видеозапись выполнена в аналоговом варианте, а другая в цифровом, эксперт вынужден использовать различные технические средства и программное обеспечение. В каждом из редакторов эксперт производит персональную обработку исходных изображений для дальнейшего изучения, которая включает методы улучшения изображений, изменения характеристик и масштаба, трансформацию формы и удаление технических недостатков, яркостно-контрастную коррекцию и т.д.

Это лишь часть функций программ, не прошедшие специальной сертификации. Профессиональные операторы использую большее количество инструментов и фильтрующих систем, вмешивающихся в содержание фото-, видеозаписей, что категорически недопустимо для судебных доказательств. Современные программные инструменты обладают негативным для правоохранительной деятельности свойством «все доступности», что позволяет трансформировать изображения объектов и проводить неконтролируемую обработку. У современной молодежи появился термин для обозначения таких манипуляций «отфотошопить» или «зафотошопить». К примеру, в интернете доступна информация, о том, как изготовить поддельный электронный общегражданский паспорт. Подобная информация предназначается для несовершеннолетних, которым требуется приобрести запрещенные товары в интернет-магазинах[4]. Полагаем, что в вопросе использования цифровых изображений следует навести порядок, и начать необходимо с создания специализированного программного обеспечения.

Другой стороной работы с доказательствами является процедура экспертного исследования визуальных изображений человека. В настоящий момент методика портретной экспертизы предполагает использование графических редакторов для применения методов сравнения и представления результатов. Наибольшей популярностью у экспертов пользуются редакторы иностранного производства, разработанные и функционирующие на алгоритмах,

не отвечающих требованиям российского законодательства[5], в соответствии с которым, специализированное программное обеспечение должно находится в едином реестре российских программ и быть адаптировано к ведомственным информационным системам. Российские программисты только недавно приступили к созданию аналогичных программ, поэтому их продукт не в полной мере отвечает заявленным требованиям. Представляется, что создаваемое программное обеспечение должно соответствовать возможностям самых передовых технологий в области цифровой обработки, как фото - так и видеоизображений, и сориентированы на потребности судебных экспертиз.

Разрабатываемые графические редакторы должны производить ввод изображений с различных регистрирующих устройств (фото, видео, сканеры и др.), обеспечивать обработку двух- и трехмерных статических изображений, двух- и трехмерные динамические изображения. Все манипуляции, начиная от ввода изображения до окончания работ с изображением по конкретному заключению эксперта, включая иллюстрационное и текстовое оформление, должны фиксироваться в журнале (протоколе) обработки и сохраняться вместе с электронными и бумажными документами, фиксирующими ход, условия и результаты исследования. Архив с электронными приложениями к заключению эксперта необходимо аккумулировать в судебно-экспертном учреждении. По требованию органа или лица, назначивших экспертизу, указанные данные предоставляются для приобщения к делу[6].

Программы для обработки изображений исследуемых объектов, должны отвечать требованиям экспертной методики конкретного вида. При этом, набор модулей и инструментов может отличаться в зависимости от профиля программы. Например, для криминалистических экспертиз следует предусмотреть варианты программ для портретной экспертизы, для трасологических и баллистических экспертиз, для технико-криминалистического исследования.

Специализированные программы, предназначенные для конкретных видов экспертной деятельности, должны обеспечивать прозрачность и воспроизводимость методов исследования в соответствии с сохраненным архивом манипуляций по обработке фото-, видеоизображений. Сохраненные в журнале обработки изображений параметры, должны быть обязательной частью экспертного заключения в соответствии с требованиями процессуального законодательства и закона о государственной судебно-экспертной деятельности.

Резюмируя сказанное, предлагаем минимально необходимый перечень модулей, которыми следует оснащать графические редакторы фото-, видеоизображений:

1. Модуль ввода изображений из разных источников.

2. Модуль хеширования цифровых изображений, поступивших на исследование с набором функций по выявлению, на предварительной стадии исследования признаков, указывающих на изменение исходного фото - или видеоизображения, полученного тем или иным техническим средством во

время съемки (изменение метаданных, вмешательством программ редактирование и т.п.).

3. Модуль количественных методов исследования, обеспечивающих проведение проверки (калибровки) измерительного инструмента в зависимости от выбранного разрешения изображения объекта исследования. Возможность проводить ручные и автоматические измерения (размеров, углов, площадей и т.п.), а также ведение журнала измерений. Соответствие проводимых измерений требованиям действующего закона[7] и подзаконных актов.

4. Модуль цифровой обработки изображений в соответствии с методикой исследования, включая инструменты, по улучшению различимости признаков объекта (специальных фотографических методов исследования).

5. Модуль анализа изображений (распознавания лиц по признакам внешности).

6. Модуль текстовой печати (текстовый редактор), обеспечивающий верстку заключения эксперта и иллюстраций с разметкой, ведения журнала редактора с последующим объединением всех журналов обработки (изображений, измерений, текстов).

7. Модуль выгрузки текста и иллюстраций в формате гарантирующим исключение внесения изменения (формат PDF, цифровая подпись и т.п.).

8. Модуль архивирования, хеширования и сохранения электронных документов для хранения в экспертном учреждении (совместимый, для единого делопроизводства в правоохранительной системе независимо от ведомственной принадлежности) в соответствии с требованиями закона.

Литература

1. Газизов В.А. Создание эффективной биометрической системы идентификации по изображению лица для МВД России - необходимость на современном этапе развития информационного общества // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: научное электронное издание (16020 Кб). – М., 2019. С. 77.

2. Белкин Р.С. Курс криминалистики: Учебное пособие для вузов. 3-е изд., доп. – М.: ЮНИТА-ДАНА. Закон и право. 2001. С. 473.

3. Исследование объектов криминалистических экспертиз методами цифровой обработки изображений // Учебное пособие / Дмитриев Е.Н., Зудин С.И., Иванов П.Ю. - М., 2000. - 80 с.

4. Онлайн юридический эксперт. Консультация адвоката. (Название страницы с сайта). Электронный ресурс. Режим доступа – свободный. Адрес: https://tul-mebel.ru/konsultatsiya-advokata/kak-otfotoshopit-pasport-na-18-let.php

5. Постановление Правительства РФ от 16.11.2015 г. N 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

6. Федеральный закон от 31.05.2001 N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Ст. 25.

7. Федеральный закон от 26 июня 2008 г. N 102-ФЗ «Об обеспечении единства измерений» Электронный ресурс. Режим доступа – свободный.

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ КИБЕРТЕРРОРИСТИЧЕСКИХ АТАК С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ ПРОГРАММ: ПРИНЦИПЫ РЕАЛИЗАЦИИ

Гайфулин Виктор Валерьевич[1], gayfulin2007@yandex.ru
Голубков Денис Александрович[2], gda9999@bk.ru
Ус Кирилл Александрович[3], uskir@mail.ru

[1]Краснодарский университет МВД России
[2]Крымский филиал Краснодарского университета МВД России
[3]Московский Государственный Технический Университет имени Н. Э. Баумана

Аннотация. Дается определение кибертерроризму как социальному явлению. Обосновывается актуальность совершенствования методов криминалистического анализа кибертеррористических атак, совершаемых с использованием вредоносных программ. Рассматривается методический аппарат функционального моделирования как источник криминалистически значимых признаков такого рода противоправных действий. В рамках рассмотренного методического аппарата приводится пример функциональной декомпозиции целевой функции злоумышленника - «Вредоносное воздействие на информацию в КС».

Ключевые слова: кибертерроризм, кибертеррорестическая атака, вредоносная программа, криминалистическое исследование компьютерных средств и систем, функциональная декомпозиция.

Расширение возможностей сетевых технологий, как предпосылки реализации методов распределенной обработки данных в компьютерных системах (КС), наряду с громадным положительным эффектом привело и к ряду негативных моментов, связанных с резким увеличением числа уязвимостей информации к реализации угроз компьютерных атак [1].

Существующая классификация компьютерных атак по тяжести воздействия на инфокоммуникационную инфраструктуру выделяет отдельный тип атак, направленных на блокирование доступа к основным узлам КС и искажение обрабатываемой информации. Цель такой атаки очевидна - парализовать работу всей инфокоммуникационной инфраструктуры.

Подобное явление имеет конкретное правовое определение - кибертерроризм [2].

Кибертерроризм, как новое социальное явление, относится к классу высокотехнологичного терроризма и представляет серьезную угрозу безопасности государств с развитой инфраструктурой информационного обмена. Потенциальными объектами кибертерроризма являются Интернет, технологии дистанционного банковского обслуживания, биржевые, архивные, исследовательские, управленческие информационные системы, средства коммуникации, электронные средства массовой информации, базы персональных данных [3]. Использование в качестве инструмента несанкционированного

доступа к информационным ресурсам КС вредоносных программ позволяет кибертеррористу соответствующей квалификации атаковать эти объекты с одного единственного компьютера.

Ассоциативность, репликативность и полиморфность являются теми характерными свойствами вредоносных программ, которые позволяют им выполнять функции несанкционированной манипуляции информацией в рабочей среде средств вычислительной техники на фоне работы программного обеспечения этих средств. Подобные свойства вредоносных программ делают их привлекательным инструментом кибертеррорестических атак, что, в свою очередь, приводит к необходимости совершенствования методологии криминалистического анализа подобного рода противоправных действий [4].

Анализ закономерностей формирования методологии нового раздела криминалистики - криминалистического исследования компьютерных средств и систем как [5] позволяет выявить устойчивую тенденцию интегрирования в рамках данного раздела как классических методов криминалистического исследования, так и методов теории системного анализа [6] и теории распознавания [7]. Криминалистическое исследование компьютерных средств и систем с целью выявления противоправных действий, совершаемых с использованием вредоносных программ [8] является наиболее характерным проявлением данной тенденции. Основополагающими методическими положениями для криминалистического анализа подобного рода противоправных действий являются:

первое – число вариантов реализации противоправных действий с использованием вредоносных программ является ограниченным;

второе – существует множество признаков распознавания воздействий вредоносных программ на информационную среду КС, адекватно отражающих реализацию этими программами своих функций;

третье - порядок реализации этих функций детерминирован.

Реализация этих положений связана со структуризацией функционального представления противоправных действий в сфере компьютерной информации с использованием вредоносных программ. Результатом структуризации является представление подобных действий в виде многоуровневой иерархической структуры функциональных состояний исследуемого процесса. При этом каждое из этих состояний является результатом детализации функциональной структуры исследуемого процесса более высокого уровня.

То обстоятельство, что действия злоумышленника при реализации им противоправных действий в сфере компьютерной информации с использованием вредоносных программ имеют целевую направленность, исследование такого рода действий методами функциональной декомпозиции связано с детализацией целевой функции «Вредоносное воздействие на информацию в КС». Процедура декомпозиции состоит в выделении функционально специализированных элементов - функций и логических связей между ними, имеющих место в процессе воздействия вредоносных программ на информацию в КС. Формируемое таким образом описание данного процесса является его функциональным представлением [9].

В основе функционального представления противоправных действий в сфере компьютерной информации с использованием вредоносных программ лежит представленное в формализованном виде описание подобного рода действий как процесса достижения определенной цели в результате выполнения целевой функции «Вредоносное воздействие на информацию в КС». Обозначим данную функцию как *Ф*. Очевидно, что степень достижения данной цели в процессе реализации подобного рода противоправных действий допускает функциональное представление, а сами функции можно представить в виде вредоносных воздействий.

Допустимость функционального представления противоправных действий в сфере компьютерной информации с использованием вредоносных программ, в свою очередь предполагает представление такого рода действий в виде упорядоченной последовательности (множества) функций, реализация которых определяет целевую функцию *Ф*.

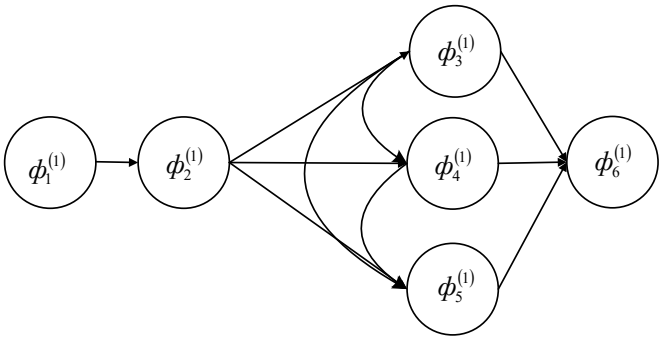
Представление целевой функции *Ф* в виде упорядоченной последовательности функций $\phi(1)j \square\ \Phi$, а каждой из функций $\phi(1)j$ - в виде упорядоченной последовательности более детализированных, по сравнению с $\phi(1)j$, функций $\phi(2)jk \square\ \phi(1)j$ и т.д. Соответствующие множества функций формируют декомпозиционный структурный базис функционального описания противоправных действий в сфере компьютерной информации с использованием вредоносных программ.

Процедура декомпозиции реализуется до тех пор пока не образуется уровень детализации, достаточный для формирования криминалистически значимого набора признаков, обеспечивающего следообразование воздействий вредоносных программ [4].

В результате анализа способов совершения противоправных действий в сфере компьютерной информации с использованием вредоносных программ, установлено, что подобного рода действия представляют собой последовательность реализации следующих этапов (рисунок 1):

- вскрытие механизмов защиты информации в КС;
- внедрение вредоносной программы в качестве ложного доверенного объекта доступа к информации в КС;
- нарушение конфиденциальности информации в КС;
- нарушение целостности информации в КС;
- нарушение доступности информации в КС;
- скрытие следов воздействия вредоносной программы на информацию в КС.

Функция Φ – «Вредоносное воздействие на информацию в КС»



$\phi_1^{(1)}$ - функция «Вскрытие механизмов защиты информации в КС»

$\phi_2^{(1)}$ - функция «Внедрение вредоносной программы в качестве ложного доверенного объекта доступа к информации в КС»

$\phi_3^{(1)}$ - функция «Нарушение конфиденциальности информации в КС»

$\phi_4^{(1)}$ - функция «Нарушение целостности информации в КС»

$\phi_5^{(1)}$ - функция «Нарушение доступности информации в КС»

$\phi_6^{(1)}$ - функция «Скрытие следов воздействия вредоносной программы на информацию в КС»

Рисунок 1.

Детализацию этапов нулевого уровня структуры функционального представления целевой функции «Вредоносное воздействие на информацию в КС» рассмотрим на примере декомпозиции функции $\phi_2^{(1)}$ - «Внедрение вредоносной программы в качестве ложного доверенного объекта доступа к информации в КС». Данную функцию составляют следующие функции первого уровня декомпозиции (рисунок 2):

- использование недостатков алгоритмов удаленного поиска;
- нарушение механизма реализации сетевого сервиса.

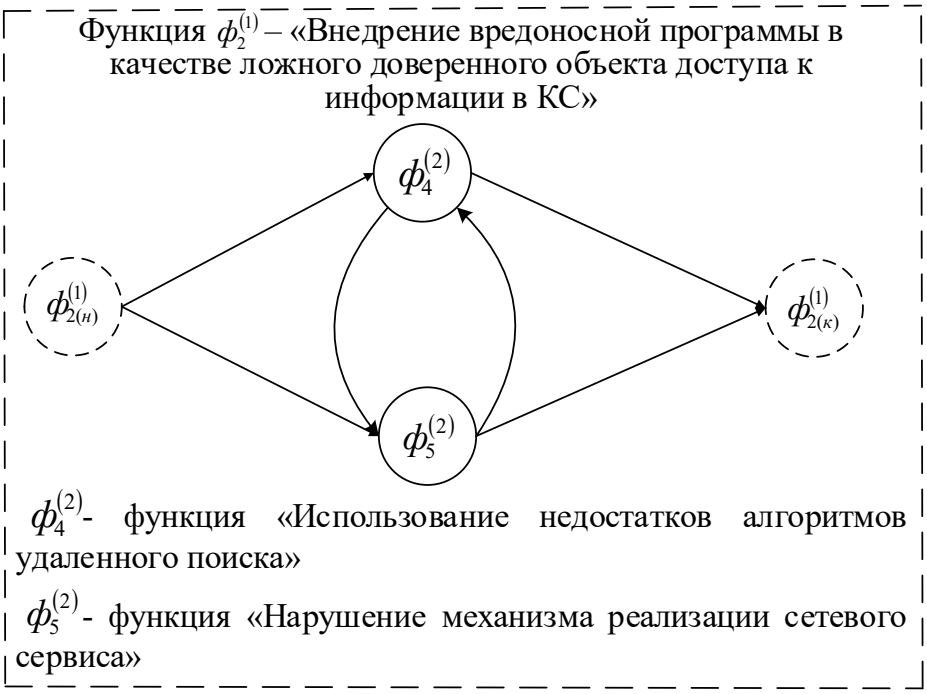


Рисунок 2

На рис. 2 $\phi_{2(н)}^{(1)}$ и $\phi_{2(к)}^{(1)}$ обозначены так называемые псевдовыполняемые начальная и конечная функции. Подобная условность графового представления обусловлена случаями, когда две функции и более являются начальными или конечными.

Детализацию функций первого уровня структуры функционального представления целевой функции «Вредоносное воздействие на информацию в КС» рассмотрим на примере декомпозиции функции $\phi_4^{(2)}$ - «Использование недостатков алгоритмов удаленного поиска». Данную функцию составляют следующие функции второго уровня декомпозиции (рисунок 3):

- использование недостатков алгоритмов удаленного поиска в сервисе DNS;

- ложная структуризация вычислительной сети КС.

Детализацию функций второго уровня структуры функционального представления целевой функции «Вредоносное воздействие на информацию в КС»рассмотрим на примере декомпозиции функции $\phi_{17}^{(3)}$ - «Использование недостатков алгоритмов удаленного поиска в сервисе DNS». Данную функцию составляют следующие функции второго уровня декомпозиции (рисунок 4):

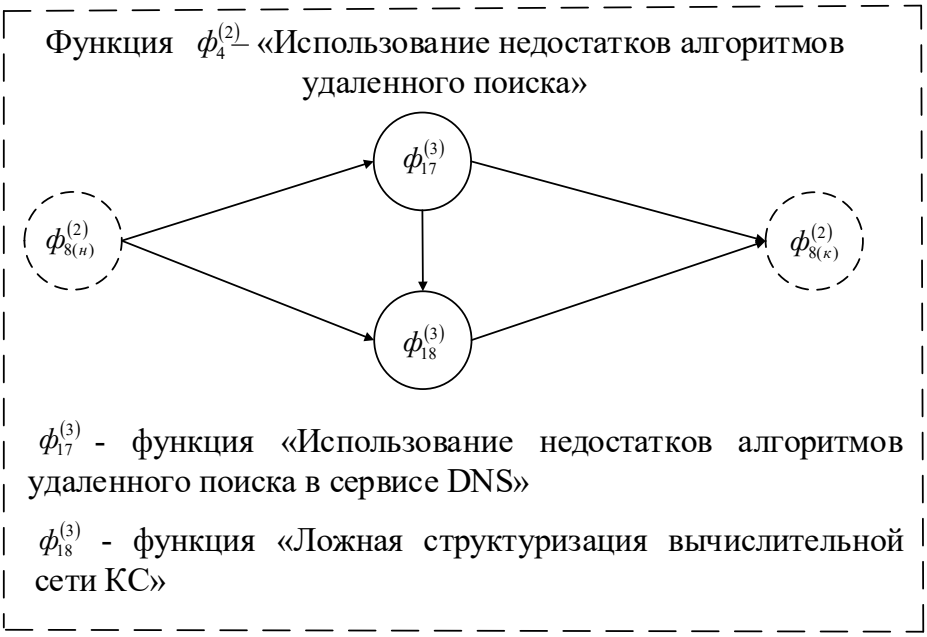


Рисунок 3

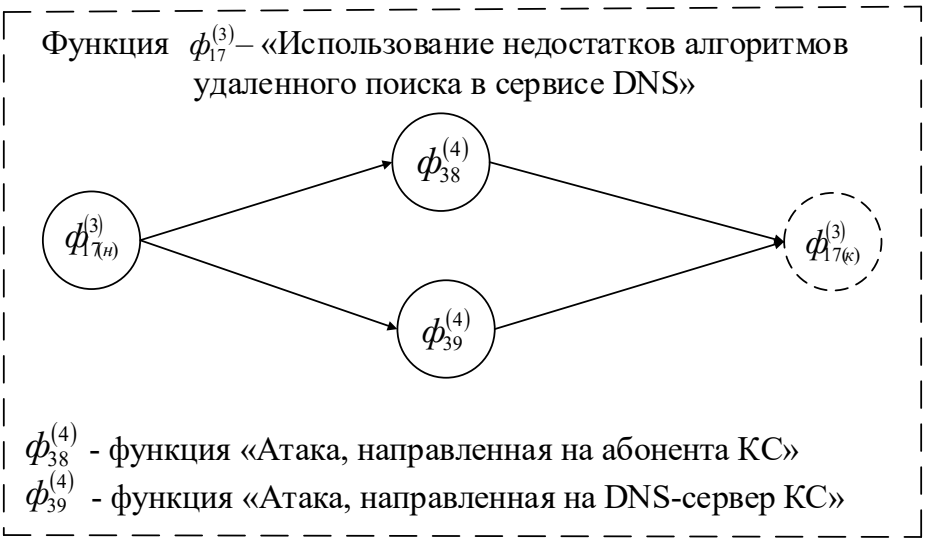


Рисунок 4.

Третий уровень декомпозиции целевой функции «Вредоносное воздействие на информацию в КС» служит основой для формирования набора первичных признаков распознавания противоправных действий в сфере компьютерной информации с использованием вредоносных программ.

Таким образом очевидно, что функциональная декомпозиция рассмотренного класса угроз безопасности информации является эффективным инструментом получения криминалистически значимых данных для достижения доказательственно-иллюстративных целей при расследовании преступлений, связанных с реализацией кибертеррористических атак с использованием вредоносных программ.

Литература

1. Безопасность операционных систем: учебное пособие для системы высшего профессионального образования / под ред. С.В. Скрыля. – М.: Издательский центр «Академия», 2020. – 359 с.

2. Правовые меры противодействия информационному экстремизму: монография / О.С. Жукова, Р.Б. Иванченко, С.В. Скрыль – Воронеж: Воронежский институт МВД России, 2008. – 214 с.

3. Скрыль С.В., Зарубин С.В. Кибертерроризм как форма проявления информационного экстремизма. // Информация и безопасность. – Воронеж: Воронежский государственный технический университет, 2009. – Вып. 1. – С. 91 - 94.

4. Скрыль С.В., Тямкин А.В., Литвинов Д.В. Исследование механизмов противодействия компьютерным преступлениям: Организационно-правовые и криминалистические аспекты: монография. - Воронеж: Воронежский институт МВД России, 2009. - 218 с.

5. Россинская Е.Р., Шамаев Г.П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Электронный научный журнал «Известия Иркутской государственной экономической академии», 2015, Т. 6, №1.

6. Скрыль С.В., Шелупанов А.А. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. – М.: Машиностроение, 2008. – 138 с.

7. Распознавание и оценка угроз информационной безопасности территориальным сегментам единой информационно-телекоммуникационной системы органов внутренних дел: теоретические и организационно-методические основы. / С.В. Скрыль, В.Д. Киселев, Т.В. Мещерякова [и др.]. – Воронеж: Воронежский институт МВД России, 2012. – 160 с.

8. Организационно-правовое обеспечение информационной безопасности: учебник / А.А. Стрельцов, Б.Н. Коробец, С.В. Скрыль [и др.]. – М.: МГТУ им. Н.Э. Баумана, 2018. – 291 с.

9. Моделирование как методология криминалистического исследования в сфере компьютерной информации / С.В. Скрыль [и др.]. // Безопасность информационных технологий. – М.: МИФИ, 2005. – № 1. – С. 57 - 61.

К ВОПРОСУ О МЕТОДИКЕ ОПРЕДЕЛЕНИЯ МОДЕЛИ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОКАЗЫВАЮЩЕГО ДЕСТРУКТИВНОЕ ЭЛЕКТРОМАГНИТНОЕ ВОЗДЕЙСТВИЕ В СЕТЯХ РАДИОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ.

Гилев Игорь Владимирович[1], gileviv@bk.ru

[1]Воронежский институт МВД России

Аннотация. В статье приведены модели возможных нарушителей, способных оказать деструктивное электромагнитное воздействие на системы связи специального назначения. Путем экспертного опроса определена наиболее вероятная модель нарушителя, которая в дальнейшем может ис-

пользоваться для разработки способов противодействия деструктивным электромагнитным воздействиям

Ключевые слова: Модель нарушителя, деструктивное электромагнитное воздействие, экспертный опрос.

В настоящее время в ОВД активное распространение получили радиосети, которые в соответствии с [1] относятся к сетям связи специального назначения (СС СН). Вместе с развитием СС СН также активно развиваются криминогенные элементы, способные оказать деструктивное электромагнитное воздействие, в результате чего, оборудование СС СН может быть выведено из строя или частично парализована его работа [2]. В связи с этим, актуальность приобретает разработка способов противодействия таким деструктивным воздействиям [3]. Однако, разработка способов противодействия деструктивным электромагнитным воздействиям невозможна без рассмотрения моделей потенциальных нарушителей. В данной статье предлагается методика определения моделей нарушителя в СС СН.

Целью определения угроз безопасности информации в СС СН является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в СС СН, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба).

Нарушитель - физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах [4].

Перейдем к детальному описанию нарушителя.

Нарушитель может характеризоваться рядом параметров, таких как [4]:

Вид нарушителя (В);

Тип нарушителя (Т);

Мотив (М);

Цель (Ц);

Техническая оснащенность (ТО);

Уровень образованности (О);

Способ совершения воздействия (С).

Таким образом модель нарушителя можно представить следующим образом: Н = {В, Т, М, Ц, ТО, О, С}.

Заранее определим способ совершения воздействия, как деструктивное электромагнитное воздействие (ДЭМВ). Нарушитель оказывающий деструктивное электромагнитное воздействие на СС СН является только внешним, не имеющим физического доступа к объектам информатизации или технической радиопередающей и приемной инфраструктуре (приемо-передающее оборудование, серверы баз данных, антенно-фидерное оборудование), т.к. проход на территорию ведомственных учреждений или арендованные поме-

щения, на которых расположено радиооборудование, ограничен и доступен только сотрудникам подразделений связи и обслуживающему персоналу, имеющему определенный допуск к таким работам, под наблюдением сотрудников ОВД. Классифицировать нарушителя, как внутреннего в данном случае не корректно, поскольку сотрудники ОВД не имеют определенной цели и мотивации к нарушению функционирования ведомственной сети радиосвязи, поскольку поддержание сети в работоспособном состоянии является их непосредственной задачей. В связи с этим, далее будет рассматриваться только внешний нарушитель. К видам внешних нарушителей могут относится:

Преступные группы, воздействующие на СС СН, преследующие цель временно парализовать работу средств связи и доступ к базам данных ради совершения преступлений, беспрепятственного передвижения из одного субъекта или населенного пункта в другой и др.

Террористически и экстремистские группировки, преследующие цель нарушение и дестабилизацию управления силами и средствами ОВД, например, при возникновении ЧС и ее ликвидации.

Внешние субъекты (физические лица) недовольные деятельностью полиции, которые в качестве мести или забавы нарушают нормальное функционирование СС СН. А также специально нанятые или завербованные лица.

Бывшие сотрудники ОВД, уволенные по не реабилитирующим обстоятельствам, считающие себя неправомерно уволенными и желающими отомстить за ущемление их прав.

Сотрудники обслуживающих и монтажно-наладочных организаций, которым не вовремя перевели денежные средства за проведенные работы или которых негативно настроили в отношении ОВД, их родные или знакомые, с которыми, по их мнению, недостаточно хорошо или справедливо было проведено разбирательство со стороны сотрудников полиции. Также сотрудники из числа обслуживающего персонала могут непреднамеренно вывести СС СН из работоспособного состояния из-за своей низкой квалификации или неправильных действий.

Данных виды нарушителей преследуют главную цель: нарушение доступности и целостности, передаваемой в СС СН информации путем временного нарушения функционирования радиосредств или полного вывода СС СН из работоспособного состояния.

Мотивацией к осуществлению данной цели являются:

Желание самоутверждения и самореализации, а также любопытство.

Получение временных преимуществ от дестабилизации системы управления и связи ОВД.

Дестабилизация функционирования ОВД.

Вывод СС СН из работоспособного состояния из мести или по политическим соображениям.

Непреднамеренный вывод СС СН из-за неправильной настройки или ремонта других радиосредств, осуществляющих работу вблизи радиооборудования СС СН.

Реализация террористического акта (электромагнитный терроризм).

Возможность реализации угроз по нарушению функционирования СС СН определяется уровнем образованности и соответствующими знаниями (компетенциями), а также техническим оборудованием, которым обладают нарушители. Классифицируя правонарушителей по уровню имеющихся знаний можно выделить следующее деление:

Нарушитель, обладающий низким уровнем знаний в области беспроводных систем связи и воздействия на них, однако его могут завербовать и произвести экспресс обучение по тому, как произвести деструктивное воздействие, с целью сокрытия истинных организаторов атак на СС СН.

Нарушитель, имеющий базовый или средний уровень осведомленности в системах связи и способах воздействия на них.

Нарушитель имеющий высокий уровень познания в радиоэлектронной борьбе и радиоэлектронном противодействии, обладающий подробными знаниями о структуре и принципах функционирования радио СС СН.

По технической оснащенности нарушители могут быть:

Оснащены самодельно спроектированными и собранными средствами радиовоздействия.

Оснащены средствами радиоподавления открыто распространяющимися на территории РФ.

Оснащены специальными техническими средствами (СТС) радиоэлектронного подавления (РЭП), отсутствующими в открытой продаже. Нарушитель использующий СТС, к таким средствам можно отнести БПЛА с комплексом радиоэлектронного подавления.

На основании вышеизложенных факторов были предложены следующие модели нарушителей:

№	В	Т	М	Ц	ТО	О	С
1	внешний	преступные группы	получение временных преимуществ от дестабилизации системы управления и связи ОВД	нарушение доступности и целостности	самодельные средства РЭП, открытые к продаже средства РЭП,	низкий или средний	ДЭМВ
2		террористические и экстремистские группировки	дестабилизация функционирования ОВД		самодельные средства РЭП, специальными средствами РЭП	базовый или средний	
3		внешние субъекты	желание самоутверждения и самореализации, любопытство, подкуп		самодельные средства РЭП, открытые к продаже средства РЭП	базовый или низкий	
4		бывшие сотрудники ОВД	месть, обида		самодельные средства РЭП, открытые к продаже средства РЭП	средний	
5		сотрудники обслуживающих и монтажно-наладочных организаций	нет цели	нет мотива нарушения нормального функционирования	самодельные средства РЭП	средний или высокий	

Для выявления типовой модели нарушителя был проведен экспертный опрос, в ходе для которого были отобраны действующие сотрудник ОВД, работающие в центрах информационных технологий, связи и защиты информации более 10 лет, имеющие высшее техническое образование. К опросу было привлечено 10 экспертов. Опрос осуществлялся путем выставления оценок каждым респондентом, предложенным моделям нарушителя. Оценки выставлялись в пределах от 1 до 5, где 1- маловероятное событие, а 5 – собы-

тие с большой степенью вероятности. Выставленные экспертами оценки приведены в табл.1.

Оценку опроса экспертов будем производить в программном продукте STATISTICA.

Табл.1 Экспертные оценки

	Модель 1	Модель 2	Модель 3	Модель 4	Модель 5
Эксперт 1	4	3	2	1	1
Эксперт 2	5	2	3	2	1
Эксперт 3	3	4	2	2	1
Эксперт 4	4	5	3	1	2
Эксперт 5	3	3	2	1	1
Эксперт 6	1	3	4	2	2
Эксперт 7	3	2	4	1	2
Эксперт 8	5	3	2	2	1
Эксперт 9	4	3	3	2	1
Эксперт 10	2	4	2	1	1

Произведем обработку оценок, выставленных экспертами, с целью выявления согласования в их оценках. Для этого обычно применяется мера согласованности экспертных мнений - дисперсионный коэффициент конкордации (коэффициент согласия) равный:

$$W = \frac{D}{\mathrm{D}_{max}}$$

где, D – оценка дисперсии, Dmax – максимальное значение оценки дисперсии. Коэффициент конкордации изменяется от 0 до 1, W=0 в случае полного расхождения между выставленными экспертами оценок, если W=1, то мнения экспертов полностью совпадают. Для нашего случая значение Вычисленный коэффициент конкордации W=0,6, что позволяет сделать вывод о достаточно высокой согласованности выставленных экспертами оценок. На основании экспертного опроса наиболее вероятной моделью нарушителя является первая.

Таким образом, в данной статье были рассмотрены возможные модели потенциальных нарушителей в СС СН, оказывающих ДЭМВ. Путем экспертного опроса была определена наиболее вероятная модель нарушителя, исходя из которой, следует осуществлять разработку способов противодействия ДЭМВ в СС СН.

Литература

О связи: федеральный закон от 07.07.2003 № 126-ФЗ: (с изм. и доп.) // «СПС КонсультантПлюс». – URL: http://www.consultant.ru /document/cons_doc_LAW_43224// (дата обращения: 01.05.2020).

Хохлов Н. С., Канавин С. В., Гилев И. В. Использование многосекторной антенной системы MIMO как элемента комплекса средств противодействия деструктивным электромагнитным воздействиям // Вестник Воронежского института МВД России. – 2019. – № 4. – С. 126–136.

1. Гилев И. В Модель противодействия разрушению информации при деструктивных электромагнитных воздействиях в системах радиосвязи специального назначения на основе нечетких экспертных систем // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 158–168.

2. Методика определения угроз безопасности информации в информационных системах. – URL: https://fstec.ru/component/attachments/download/812// (дата обращения: 01.05.2020).

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ НА ПУТИ К ИНТЕЛЛЕКТУАЛЬНОМУ ЗДАНИЮ

Гречаный Сергей Анатольевич[1], grechan7777@mail.ru
Романов Михаил Сергеевич[1], m.romanov90@mail.ru
Таравков Михаил Владимирович[1], berloga_@rambler.ru

[1]Воронежский институт МВД России

Аннотация. В статье рассмотрены вопросы применения интегрированных систем безопасности на объектах различного назначения. Показаны преимущества интеграции отдельных подсистем, приведены примеры практической реализации. Рассмотрены тенденции, проблемы и перспективы развития интегрированных систем безопасности до уровня интеллектуальных зданий, интеллектуального города.

Ключевые слова: безопасность, угроза безопасности, автоматизированная система, интегрированная система безопасности, интеллектуальное здание.

В настоящее время практически все современные объекты недвижимости независимо от их функционального назначения (жилые, офисные, производственные, транспортные, образовательные, торговые и развлекательные, здравоохранения) оборудуются различными инженерными системами для обеспечения их нормального функционирования. К таким системам относятся системы освещения, вентиляции, тепло-, газо-, электро-, водоснабжения и канализации, безопасности. Учитывая уровень криминогенной обстановки, степень важности и значимости материальных ценностей, жизни и здоровья посетителей и персонала объекта наряду с перечисленными системами системам безопасности отводится особая роль. Преступные посягательства на объект могут привести не только к материальному ущербу, нарушению функционирования объекта в целом, но и к более тяжким последствиям в виде причинения вреда жизни и здоровью людей. Помимо криминогенных и террористических угроз имеют место быть и угрозы технологического характера, такие как пожары, утечки воды и газа, нарушения электроснабжения и т.д. Для предупреждения угроз перечисленные инженерные системы могут выполнять свои функции самостоятельно без взаимодействия с другими системами. Однако эффективность и надежность их работы становится выше, когда эти системы функционируют согласованно [1]. Принимая во внимание сложность каждой из систем в отдельности, необходимость участия человека

(так как не все функции выполняются автоматически и системы имеют конечную надежность) становится актуальной задача их централизованного контроля и управления для поддержания работоспособности и принятия решения в нештатной ситуации. В таком случае наиболее рациональным решением данной задачи представляется создание единого аппаратно-программного комплекса контроля и управления с общим для всех систем диспетчерским центром. Подобные системы получили общее название SCADA систем (от английского Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных). Применительно к перечисленным выше объектам совокупность подобных систем называют интеллектуальным зданием (ИЗ), понимая под ним интеллектуальную систему [2]. Конечно, речь не идет об интеллекте, подобном человеческому. Используя термин «интеллектуальное здание» в первую очередь подразумевают способность системы анализировать происходящие события на основе количественных показателей и адаптироваться для повышения эффективности функционирования.

Для защиты объекта, персонала и посетителей от криминальных, террористических и технологических угроз в настоящее время применяется широкий спектр технических средств охраны, входящих в состав систем охранно-пожарной и тревожной сигнализации, контроля и управления доступом, охранного телевидения. Данные системы наряду с инженерными системами здания также могут функционировать самостоятельно, но, как и в предыдущем примере, эффективность их работы возрастает в результате интеграции. В результате технические средства охраны объединяются в комплексные и интегрированные системы безопасности (ИСБ) [3, 4]. Интеграция может осуществляться посредством проводных и беспроводных линий связи [5].

Первые ИСБ содержали в своем составе только технические средства охраны. В дальнейшем, по мере развития технологий, совершенствования элементной базы, программного обеспечения появилась идея расширения функциональных возможностей ИСБ, выходящих за пределы охранных функций. Существующие в настоящее время на рынке ИСБ все без исключения позволяют осуществлять контроль и управление различными инженерными системами. В связи с этим можно отметить две тенденции в построении интеллектуального здания: включение функций безопасности в системы автоматизации и диспетчеризации зданий и развитие ИСБ до систем интеллектуального здания. В целом разделение этих направлений достаточно условно, и в основном это связано с тем, какие задачи ставились первоначально при разработке системы. В России задачи построения систем безопасности всегда имели приоритет, и, соответственно, второй путь получил большее развитие.

На фоне общего развития науки и техники в последнее время наблюдается повышенный интерес разработчиков и пользователей систем промышленной автоматизации к интеграции систем автоматизации и диспетчеризации с системами безопасности зданий. Такая тенденция, с одной стороны, может быть обусловлена возрастающими требованиями к уровню обеспече-

ния безопасности. С другой стороны, развитие систем безопасности привело к созданию интегрированных систем, которые объединили в своем составе ранее уже функционирующие охранную и пожарную сигнализации, системы контроля и управления доступом, охранного телевидения. ИСБ позволяют вывести обеспечение безопасности на новый уровень, повысить эффективность использования организационных и технических ресурсов служб безопасности, предоставляют возможность объединить все инженерные системы объекта.

Системы безопасности развиваются неразрывно с системами обеспечения функционирования объекта, что в конечном счете приобретает более глобальный характер. Такие процессы продолжаются на протяжении нескольких лет и в конечном итоге привели к созданию интегрированных систем всего здания. Как и в случае интегрированных систем безопасности интегрированные системы зданий строятся на единой аппаратно-программной платформе, представляющей собой автоматизированную систему, элементы которой образуют многоуровневую сетевую структуру (подобно локальной вычислительной сети). Источником информации для единого центра управления являются различные сенсоры (извещатели охранной и пожарной сигнализации, датчики движения, температуры и влажности, давления, скорости ветра и т.п.), которые передают значения количественных параметров через контроллеры различных уровней и линии связи для выработки управляющего воздействия в ручном или автоматическом режиме.

Понятие «интеллектуальное здание», в отличии от «интегрированная система безопасности», в настоящее время не имеет четкого определения на уровне стандартов или иных нормативных документов. Большинство специалистов, работающих в данной области, по-своему толкуют это понятие, исходя из особенностей своей деятельности, предлагаемых решений, технических средств. Однако специалистам, занимающимся проектированием систем интеллектуального здания, нужны строго и однозначно определенные термины, требования и характеристики для разработки технической, проектной и эксплуатационной документации, а для этого, в свою очередь, необходимы стандарты и нормативные документы.

По своей сути системы ИЗ представляют собой автоматизированные системы управления (АСУ), обеспечивающие управление функционированием, жизнеобеспечением и безопасностью объектов. Подобные автоматизированные системы (АСУ ФЖБ) создаются для различных объектов, от крупного предприятия до квартиры, и поэтому значительно отличаются по сложности, стоимости и функциональным возможностям. Однако принципы их построения сходны и были достаточно подробно изложены в различных публикациях.

Для пояснения понятия ИЗ можно определить, что ИЗ как и ИСБ представляет собой интегрированную автоматизированную систему, следовательно, на нее в полной мере должны распространяться положения стандартов и руководящих документов на автоматизированные системы. Например, в [6] даны следующие общие понятия.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Интегрированная автоматизированная система (ИАС) – совокупность двух или более взаимоувязанных АС, в которых функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС.

Далее приведем определения ИСБ. В [3] ИСБ называется разрабатываемая специализированная сложная техническая система, объединяющая (интегрирующая) на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных целевые функциональные технические подсистемы и технические средства, предназначенные для комплексной защиты объекта от нормированных угроз различной природы возникновения и характера проявления. В [4] ИСБ называется система безопасности объекта, объединяющая в себе целевые функциональные системы, предназначенные для защиты от угроз различной природы возникновения и характера проявления.

Рассматривая дальнейшую интеграцию ИСБ с инженерными системами объекта, можно предложить следующее определение термину «интеллектуальное здание».

Интеллектуальное здание – сложная техническая система, объединяющая инженерные системы здания для обеспечения его эффективного функционирования и комфортного пребывания людей, имеющая общую информационную среду и базу данных.

Интеллектуальное здание как система, построенная путем интеграции систем безопасности и инженерных систем, дает возможности решать следующие задачи:

своевременно обнаруживать и устранять аварийные и нештатные ситуации (проникновение, пожар, утечки воды, газа и т.п.), тем самым снижать их негативные последствия;

оптимально использовать силы служб безопасности для минимизации затрат и влияния человеческого фактора;

максимально эффективно управлять инженерными системами для сокращения объема потребляемых ресурсов (электрической и тепловой энергий, газа, горячей и холодной воды, воздуха и т. д.) за счет адаптации режимов функционирования инженерных систем к условиям окружающей среды;

анализировать работу инженерного оборудования и действия обслуживающего персонала и сотрудников служб безопасности для привлечения их к ответственности в случае возникновения нештатных ситуаций.

Основное предназначение интеллектуального здания – обеспечение эффективного взаимодействия всех инженерных систем, энергосбережение, предотвращение, обнаружение и своевременное реагирование на экстремальные ситуации с целью их разрешения, возникающие в процессе эксплуатации здания при максимальном снижении возможного ущерба.

Понятие «интеллектуальное здание» является относительно новым и чаще всего применяется к объектам жилищного фонда и офисам. В случае использования таких систем на промышленных и производственных объектах появляется возможность автоматизации производственных (технологических) процессов наряду с защитой объекта и персонала от различных угроз, в том числе техногенного характера, которые могут возникнуть в процессе функционирования объекта. Взаимодействие систем безопасности, инженерных систем (жизнеобеспечения) и систем автоматизации позволяет эффективно решать стоящие перед объектом задачи. Поэтому предлагается называть такие системы автоматизированными системами управления функционированием, жизнеобеспечением и безопасностью объекта (АСУ ФЖБ).

Сравнительный анализ принципов построения ИСБ и ИЗ, в состав которых может входить оборудование разных производителей, позволяет сделать вывод о том, что они строятся на основе общих принципов. Основными структурными элементами таких систем являются специализированные вычислительные устройства – контроллеры, которые посредством линий связи объединяются в сети разного уровня сложности наподобие CAN (от англ. Controller Area Network – сеть контроллеров). В крупных и масштабируемых системах используется многоуровневая иерархическая структура сетевого взаимодействия.

Подводя итог можно отметить, что развитие ИЗ в настоящее время происходит в более широких масштабах, выходя за рамки рассмотренной АСУ ФЖБ объекта. Кроме рассмотренных инженерных систем в состав ИЗ могут входить системы связи, защиты информации, развлечения и т.п. Возможность расширения ИСБ до масштабов ИЗ зависит от потребительского спроса, развития технологий и экономической эффективности. В дальнейшем очередным шагом в развитии ИЗ может быть создание систем «интеллектуальный город», что с учетом развития АПК «Безопасный город» в соответствии с Концепцией [7] имеет широкие перспективы в России.

Литература

1. Рогожин А.А. Моделирование и оценка надежности интегрированной системы безопасности административного здания // А.А. Рогожин, М.В. Таравков. Фундаментальные проблемы системной безопасности: сборник материалов школы-семинара молодых ученых, посвященной 60-летию запуска первого в мире искусственного спутника Земли: Севастополь. – Цифровая полиграфия, 2017. – С. 238-248.

2. ГОСТ Р 56875-2016. Информационные технологии (ИТ). Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий. – Введ. 2017-01-01. – Москва: Стандартинформ, 2019. – 64 с.

3. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. – Введ. 2010-09-01. – Москва: Стандартинформ, 2010. – 62 с.

4. ГОСТ Р 57674-2017. Интегрированные системы безопасности. Общие положения. – Введ. 2018-06-01. – Москва: Стандартинформ, 2019. – 13 с.

5. Горшков И.Ю. Анализ технических решений в области программно-аппаратной интеграции радиоканальных и проводных подсистем ИСБ / И.Ю. Горшков, М.В. Таравков

// Сборник материалов Всероссийской научно-практической конференции «Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем». – Воронеж: Воронежский институт МВД России, 2016. –С. 21-22.

6. ГОСТ 34.003-90. Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – Введ. 1992-01-01. – Москва: Стандартинформ, 2009. – 48 с.

7. Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» [Электронный ресурс: Распоряжение Правительства РФ от 03.12.2014 № 2446-р (ред. от 05.04.2019). – Режим доступа: Система «Консультант плюс».

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

Данилов Роман Михайлович[1], danilovroman@mail.ru
Рыбак Александр Владимирович[1], rybak_2908@mail.ru

[1]Дальневосточный юридический институт МВД России

Аннотация. В статье рассматриваются виды проявления экстремизма в сети Internet, а также способы его выявления и профилактики.

Ключевые слова: экстремистская деятельность, интернет, электронные средства передачи информации.

В последнее время в России наблюдается всплеск экстремизма. В средствах массовой информации неизменно «крутят» новости о террористических группировках, религиозно - политическом экстремизме и терроризме в целом.

Надо признать, что в молодежной среде подобные проявления распространены особенно. В первую очередь это связано с тем, что именно данной социально-возрастной группе, как никакой иной, свойственны такие качества как максимализм, подражание, резкость и непреклонность в суждениях и поступках. Ложные жизненные ориентиры также зачастую выражаются в пренебрежении к действующим в общественном пространстве законам, правилам и нормам поведения. Все это в последствии приводит к массовому молодежному экстремизму.

Как известно, основной целью экстремизма является навязывание определенных убеждений населению и привлечение как можно большего числа единомышленников в свои организации. Возникает вопрос, где это можно сделать в современном информационном обществе?

В наши дни информационное пространство сети Интернет используют различные экстремистские и террористические организации, радикально настроенные группировки с целью вербовки молодежи для претворения в жизнь идеологии экстремистской направленности. Распространение молодежного экстремизма в сети Интернет является острой проблемой для «мир-

ных» граждан. Увеличивается количество преступлений, поднимается уровень насилия, экстремизм становится более жестоким и профессиональным. Данный вид экстремизма можно определить, как информационный экстремизм [1].

С целью противодействия этому проявлению 28 ноября 2014 года Президентом Российской Федерации был подписан Указ № Пр-2753 «О внесении изменений в Стратегию противодействия экстремизму в Российской Федерации до 2025 года», разработанный Министерством внутренних дел [3].

Как следует из документа, спецслужбы иностранных государств и некоторые зарубежные организации стремятся дестабилизировать ситуацию в России, для чего усиливают свое влияние на молодежь посредством наращивания информационно-психологического воздействия и разрушения традиционных российских духовно-нравственных ценностей. Как правило, они действуют под видом культурных, образовательных, гуманитарных, национальных и религиозных проектов. Распространяя ложные сведения о политических, социально-экономических, экологических и иных условиях развития страны, они стремятся повлиять на мировоззрения молодых людей, посеять в их умах сомнения в правильности принимаемых решений руководством страны, руководителями исполнительной и законодательной властей, деятелями культуры и сторонниками различных религиозных конфессий. И в конечном итоге – дестабилизировать ситуацию, сначала в определенном регионе России, а затем и целиком в стране, создать и усилить протестные настроения. Именно так следует расценивать их возросшую активность в подстрекании населения к протестным акциям и навязыванию людям своего, строго определенного сценария развития событий, неоднократно опробованного на территории других государств.

Министерство МВД заявляет, что радикализм затрагивает и спортивное сообщество России. «Серьезную опасность представляет распространение радикализма в спортивной среде, в том числе на базах спортивных школ и клубов, а также проникновение в тренерско-преподавательский состав носителей экстремистской идеологии», – отмечают составители документа.

Проявляется это в несанкционированных акциях протеста и организацией массовых беспорядков, что, бесспорно, является серьезным фактором дестабилизации общественно-политической обстановки. Одним из основных способов проявлений такой деятельности является привлечение различных групп населения к участию в несогласованных публичных массовых мероприятиях, которые, затем, умышленно трансформируются в массовые беспорядки.

МВД РФ, являясь разработчиком проекта указа, также подчеркивает, что участившиеся случаи вовлечения несовершеннолетних лиц в ряды экстремистки настроенных структур, представляя серьезную угрозу обществу, так как данная категория легче всего поддается идеологическому и психологическому воздействию. И одновременно в ряде случаев не подлежит уго-

ловной ответственности. С целью противодействия этому явлению авторы проекта предложили изменить саму стратегии работы с молодежью. А именно – включить в региональные и муниципальные учебные программы по образованию и воспитанию детей ряд мероприятий по формированию у подрастающего поколения уважительного отношения к своим родителям, учителям, старшим товарищам и пожилым людям, а также всем существующим религиям и представителям других национальностей с их традициями и обрядами.

Были предложены также мероприятия по организации досуга детей, созданию нормальных условий для занятия спортом, посещения различных кружков и секций с целью раскрытия творческого и спортивного потенциала подростков, а также созданию условий для их активного отдыха.

Выполнить эти условия крайне важно, так как в настоящее время в различных регионах России фиксируются попытки создания глубоко законспирированных ячеек экстремистских и террористических организаций с вербовкой и обучением все новых и новых участников. Учеба в них, зачастую, осуществляется дистанционно. Посредством таких действий и происходит распространение крайне радикальных взглядов среди приезжающих в Россию трудовых мигрантов, вовлечение их в преступные группировки и организация различных структур с экстремистской и террористической направленностью. Как утверждают эксперты МВД, возникновению в ряде регионов страны данных проявлений способствуют обострившиеся в последнее время миграционная обстановка, выразившаяся в дестабилизации рынка труда. Все это самым негативным образом влияет на межрелигиозные и межнациональные отношения между людьми, приводит к вражде и ненависти друг к другу.

«Сохраняющиеся очаги терроризма, межнациональной розни, религиозной вражды и иных проявлений экстремизма, прежде всего на Ближнем Востоке и в Северной Африке, способствуют проникновению в миграционные потоки членов международных экстремистских и террористических организаций, а также распространению экстремистской и террористической идеологии и пропаганды, в том числе в сети Интернет», - отмечают эксперты МВД России. Их озабоченность вызывает и проникновение в РФ представителей радикальных религиозных течений из других государств, выпускников зарубежных теологических центров, проповедующих исключительность таких религиозных течений и насильственные методы их распространения.

В указе президента РФ в сфере миграционной политики предлагаются меры по совершенствованию социальной и культурной адаптации иностранных граждан. А также их скорейшая интеграция в общественные процессы страны пребывания, для чего предусматривается обязательное вовлечение потенциальных работодателей, получающих квоты на привлечение иностранной рабочей силы, в работу по реализации и финансированию социальных и культурных программ.

В документе указывается на необходимость принятия жестких мер по противодействию незаконной миграции, профилактике, выявлению и пресечению правонарушений в сфере миграции и привлечение к ответственности виновных лиц. Специалисты МВД России предлагают также обеспечить «противодействие формированию этнических анклавов, социальной исключительности отдельных групп граждан по признаку социального, культурного, расового, национального или религиозного отличия, а также их пространственной сегрегации».

Для обеспечения незамедлительного реагирования на факты распространения экстремистской идеологии и выявления материалов, направленных на подготовку и совершение экстремистских и террористических актов, в сфере государственной информационной политики авторы проекта предлагают осуществлять мониторинг СМИ и информационно-телекоммуникационных сетей, включая сеть «Интернет», а также совершенствование процедуры ограничения доступа на территории РФ информационных ресурсов, распространяющих экстремистскую и террористическую идеологию.

Общеизвестно, что сеть Интернет является идеальным инструментом пропаганды для террористов и экстремистов, поскольку располагает рядом важных характеристик, которыми активно пользуются бандформирования и иные структуры экстремистского и террористического толка. А именно:

– широкий охват аудитории;
– анонимность размещения информации;
– высокая скорость распространения материалов;
– возможность анонимного создания собственных пропагандирующих интернет-ресурсов без дополнительных финансовых затрат;
– наличие в законодательствах стран мира в области «компьютерного права» [8] определенных юридических лазеек и несогласованность действий в отношении экстремистских и террористических группировок.

Важно также отметить и такие преимущества глобальной сети как открытость и отсутствие цензуры. Благодаря этому появляется отличная возможность для навязывания аудитории ложных моральных ценностей и открытой свободной пропаганды религиозного экстремизма, терроризма и сепаратизма. Ведь все подобные интернет-ресурсы осуществляют свою работу из-за рубежа и имеют международные доменные имена, а именно: «.com», «.org», «.info» [7].

Наиболее распространенным для России является сайт чеченских сепаратистов «Кавказ-Центр», который долгие годы работал на американских и шведских серверах.

С целью вербовки и создания положительного и романтического образа участника подобных организаций используются наиболее популярные социальные сети и ресурсы: ВКонтакте, Одноклассники, Twitter, Youtube, Instagram. А в процессе своей деятельности активно применяется практически весь комплекс имеющихся технических возможностей по распростране-

нию информации – размещение видео- и аудиоматериалов, фотографий и документов, рассылки и «перепосты».

Данные источники являются носителями «вредительских» сведений. В своих трудах В.Н. Лопатин упоминает о видах такой информации. Так, в понимании автора к «вредоносной информации» относится:

1) информация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду;

2) призывы к войне;

3) пропаганда ненависти, вражды и превосходств;

4) посягательство на честь, доброе имя и репутацию человека;

5) информация, оказывающая разрушающее воздействие на психику людей [9]. Электронные средства являются самыми современными каналами передачи информации. И потому экстремистские организации при вербовке в свою сеть новых членов широко используют Интернет.

Чтобы противостоять этому, необходимо научиться из огромного потока информации отфильтровывать ту, что является экстремистской и направлена на организацию и создание террористического подполья. По мнению специалистов МВД России, сегодня можно выделить, как минимум, три направления в экстремисткой деятельности при осуществлении вербовки:

официальные сайты экстремистских и террористических организаций;

социальные сети, всевозможные блоги и форумы, распространяющие экстремистские материалы и инициирующие их обсуждение;

Интернет-сообщества и чаты, на которых в скрытом режиме обсуждаются планы и действия уже созданных группировок.

С приходом в нашу жизни Интернета религиозно-политические и экстремистские движения, различные группы и течения получили реальную возможность не только публично отстаивать свою идеологию и убеждения, но и вступать в дискуссии, навязывать свое мнение и взгляды аудитории, численность которой достигает десятки, а то и сотни тысяч человек.

Причем, подобные действия не всегда адекватно воспринимаются обществом и, что особенно важно, почти не контролируются государством. А вот степень их воздействия на молодежное сознание просто колоссальна, что и позволяет вербовать в ряды экстремистов и террористов все новых и новых сторонников.

Экстремистские и террористические организации рассматривают информационный экстремизм как основной способ пополнения числа своих сторонников. Контакты в Интернет-сообществах позволяют оперативно поддерживать связь на географически больших расстояниях, обсуждать, планировать и координировать будущие акции в достаточно скрытом режиме.

На сегодняшний день серьезную опасность для общества представляют сайты, откровенно проповедующие идеи экстремизма и терроризма. Через такие ресурсы международные террористические организации практически беспрепятственно осуществляют пропаганду радикальных течений ислама,

проповедующих борьбу с «неверными», «создание всемирного халифата» и т.д.

Необходимы средства для борьбы с проявлением экстремизма в Интернете. В российском законодательстве используются соответствующие нормы в уголовном и административном кодексах [6].

Чтобы противостоять подобным явлениям важно вовремя провести мероприятия по блокированию малейших проявления экстремизма. А для этого предстоит большая работа по совершенствованию нормативно-правовой базы, активизированию идеологической работы и укреплению деятельности спецслужб [5].

Таким образом, отдельные проявления экстремизма, сопряженные с использованием вредоносной информации, представляют реальную угрозу информационной безопасности не только обществу, но и государству. Экстремистская деятельность в сети Интернет может и должна рассматриваться как проблема общегосударственного значения, несущая угрозу национальной безопасности страны. Практически во всех странах мира ведется интенсивная борьба против информационного экстремизма, но актуальным остается вопрос об эффективности работы.

Литература

1. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) «О противодействии экстремистской деятельности» [Электронный ресурс] // URL: http://www.consultant.ru/ (дата обращения: 10.05.2020)

2. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // URL: http://www.consultant.ru/ (дата обращения: 10.05.2020)

3. «Стратегия противодействия экстремизму в Российской Федерации до 2025 года» (утв. Президентом РФ 28.11.2014 № Пр-2753) [Электронный ресурс] // URL: http://www.consultant.ru/ (дата обращения: 10.05.2020)

4.Борисов, С.В. Сущность преступлений экстремистской направленности / С.В. Борисов / / Мировой судья. - 2009. - №4. - С. 12 - 15.

5. Валеев, А.Х. Борьба с проявлением экстремизма в сети интернет / А.Х. Валеев // Бизнес в законе. - 2011. - №6. - С. 125.

6. Герасимов, Б.М. Проблемы российского информационного законодательства / Б.М. Герасимов // Информационные ресурсы России. - 1996. - № 6. - С. 12.

7. Доника Е.Е. О некоторых проблемах противодействия экстремизму в России на современном этапе / Е.Е. Доника // Труды Академии управления МВД России. - 2008. - №3. - С. 6 - 8.

8. Кубякин Е.О. Основания социологического обоснования феномена экстремизма / Е.О. Кубякин // Экстрем-парантность: монография. - Краснодар, 2014.

9. Лопатин В.Н. Понятие и структура информационно-психологической безопасности / В.Н. Лопатин // Право и политика. - 2001. - № 10.

ФЕЙКОВАЯ ИНФОРМАЦИЯ И БЕЗОПАСНОСТЬ ОБЩЕСТВА

Бегларян Маргарита Евгеньевна[1], rita_beg@mail.ru
Демьяненко Кристина Витальевна[1], kristina-dem2011@mail.ru

[1] Северо-Кавказский филиал (г. Краснодар) ФГБОУВО
«Российский государственный университет правосудия»

Аннотация. В статье рассматриваются проблемы информированности современного общества, распространение фейковых новостей, в связи с которыми могут возникнуть проблемы с безопасностью социума и государства. Рассмотрено законодательство, которое регулирует информационные потоки и предлагается разработать комплексные меры для борьбы с вымыслами.

Ключевые слова: безопасность, информация, классификация, новость, социальная сеть, Интернет, фейк.

В настоящее время государство ужесточает меры за распространение ложной информации . Конституцией РФ гарантируется свобода мысли и слова, а также право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. [1].

Фейк на первый взгляд кажется субъективной вещью и не требует изучения. Во все времена общество вырабатывает больше информации, чем человек в состоянии переработать, поэтому такое явление, как фейковая информация, не новы, но объёмы этого социального явления увеличиваются фантастическим образом.

Такое понятие как «фейк» (от англ. fake - «подделка», «фальшивка», «обман») включает в себя ряд самых разнообразных явлений медиасреды: от поддельных текстов, а также фото-, аудио- или видеозаписей до искусственно созданной «востребованности» человека, проекта (как правило, на помощь приходят интернет-боты и/или те же фальшивые аккаунты, выставляющие «лайки» и публикующие одобрительные комментарии) [2].

На первый взгляд такие новости похожи на обычные, особенно стилистически, но отличаются от них полной или частичной недостоверностью. Исследование посвящено той части медиапространства, которое не подчиняется Закону «О средствах массовой информации» [3], каналам распространения информации, не имеющим специальной аккредитации или лицензии на введение журналисткой деятельности. Конечно, «фейки» могут присутствовать и в СМИ, но они регулируются соответствующим законодательством. Ложные новости и материалы заполоняют современное медиапространство и являются значимым фактором в насаждении тех или иных мыслей в обществе.

Мое исследование посвящено недостоверным информационным потокам, представляющим социальную значимость, информационным каналам, которые не подчинены Закону «О средствах массовой информации», а также

ФЗ от 13.07.2015 № 264-ФЗ «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации» (Закон «О праве на забвение»), призванный защитить неприкосновенность частной жизни и персональные данные граждан [4].

По сути фейковые известия тоже являются «новостями». Такие сведения привлекательны: пикантным характером, эпатажем и креативностью. Они всегда будут иметь определенный успех у людей. Исследования показывают, что аудитория зачастую предпочитают реальной новости фейковую, преувеличенную и раздутую, отличающуюся, например, катастрофизмом или большей сенсационностью [5].

Таким образом «горе-журналисты» быстро распространяют ложную информацию или измененный материал, формируя свою или заказанную картину произошедшего или несуществующего события. Делается это для увеличения продаж, коммерческого продвижения, оговора или с целью забавы.

В ноябре 2019 года Роскомнадзор (далее РКН) опубликовал первую версию открытого списка интернет-страниц, на которых регулярно официально распространяется именно ложная общественно-значимая информация. В таблицу РКН включены информационные различные источники, блоги, группы в социальных сетях (Facebook, ВКонтакте), а также каналы на YouTube.

Каждый источник из этой таблицы неоднократно был упомянут в исполнительных документах Генеральной Прокуратуры РФ, направленных в РКН, для того, чтобы исполнения положений ст. 15.3 Федерального закона №149-ФЗ «Об информации, информационных технологиях и защите информации»[6] в части, касающейся распространения недостоверной общественно значимой информации [7].

В конце 2019 года в ходе опроса граждан выяснилось, что абсолютное большинство россиян ничего не знает о законах, предусматривающих наказание за распространение лживой информации. Объясняют это тем, что эти проблемы их не затрагивают.

Для того чтобы оградить государство от потока лживой и провокационной информации о власти, чиновников и членов их семей был принят ФЗ от 18.03.2019 № 30-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» [8], прозванный в народе законом «об оскорблении власти».

Был проведен опрос для того, чтобы понять, какова реакция граждан на нововведения со стороны государства. О своей информированности заявили всего 18% респондентов. Примерно 40% отметили, что «кое-что» слышали, а 41% опрошенных услышали об этом впервые[9]. Стоит отметить, что после принятия данного закона количество клеветнических высказываний в адрес власти действительно значительно снизилось.

В настоящее время всё новостное пространство сосредоточено вокруг пандемии COVID-19. Это дало плодотворную почву для развития искажён-

ной информации. Из-за пандемии и новости о ней распространяются со скоростью вируса.

На фоне этого было принято решение в кратчайший срок внести в Уголовный и Уголовной-процессуальный кодексы РФ изменения в части уголовной ответственности за распространение недостоверной информации о COVID-19, которые 1 апреля подписал Президент РФ Владимир Владимирович Путин. Максимальное наказание по статье 207.1 УК РФ — пять лет лишения свободы [10].

В социальных сетях на волне паники о COVID-19 появились текстовые- видео- и аудиосообщения о неких ужасах, которые происходят в мире, о необходимости срочно подготовиться к «вирусной войне» и «концу света».

В Роскомнадзоре предупредили – за фейковую информацию о коронавирусе в отношении распространителей будут применены самые суровые меры. Социальные сети аккумулировали всё то, что в последнее время вызывает опасения у граждан на фоне паники из-за коронавируса. Чтобы успокоить граждан и разоблачить неверную информацию, такие новости, искажающие реальное положение вещей. собираются в единые списки и транслируются по официальным каналам.

В качестве примера рассмотрим уголовное дело из Санкт-Петербурга о распространении недостоверной информации про COVID-19. Его завели в отношении девушки-активистки, в связи с сообщением, выставленным в группе «Новости Сестрорецка» социальной сети «ВКонтакте». Информация порочит действия властей и несоблюдение санитарно-эпидемиологического режима [10]. Следствие выясняет, кто мог быть автором этого текста, и является ли владелец страницы создателем данного сообщения.

В ходе своей работы следствие сталкивается с привычными для подобных статей сложностями лингвистической экспертизы и доказательства умышленной клеветы. В первую очередь поэтому в законодательстве надо чётко дефиницировать понятие фейка, ведь до сих пор ни в одном из законов касательно защиты информации или информационной безопасности нет чёткого определения клевете или недостоверной информации.

Ложной информацией (фейком) – будем называть общедоступную информацию, распространяемую неофициально, не через СМИ, содержащую ту степень искажения реальности, которая способна нанести вред человеку, обществу или государству. Это не законченный вариант определения и он нуждается в наборе более четких признаков.

Во-вторых, необходима классификация по степени социальной значимости и лживости фейковой информации. Я предлагаю классифицировать «лживые» новости следующим образом:

В зависимости от соотношения достоверной и недостоверной информации в тексте [11]:

1. «Новость» представляет собой ложь. Создатель такого текста понимает социальную значимость содеянного.

2. Достоверная информация раскрашена недостоверными красками, правда и ложь переплетаются между собой.

3. В заведомо ложную картину событий вплетены незначительные правдивые факты или события, которые не являются определяющими.

Далее ложную информацию нужно классифицировать по уровню социальной значимости, а именно:

1. Общественная, которая затронет большинство людей. Такая новость социально значима для государства и может представлять большую опасность.

2. Индивидуальная, которая касается только одного человека и возможно его семьи.

Фейковая новость, которая имеет социальную значимость, должна быть обязательно опровергнута. Необходимо отметить, что недостоверные новости не несут вреда, если они: не оскорбляют власть, не переписывают историю, не призывают к насилию и не представляют опасности для бизнеса.

Предложенные классификации могут стать основой для ранжирования наказания за неправдивую информацию.

Один из лучших способов остановить увеличение дезинформации - это научить слушателей оценивать новости, которые им преподносят современный информационный мир, но это утопия.

Поэтому властям в свою очередь необходимо отслеживать выставленные на всеобщее обозрения новости и предпринимать меры по устранению ложных источников. Прошу не путать данный процесс с цензурой. Так как в соответствии с п.5 ст. 29 Конституции РФ цензура запрещена.

Например, есть специальные ресурсы, на которых можно найти первоисточник фотоизображения: Findexif. com, Fotoforensics.com и др. [12].

Также можно доработать методы и критерии независимой лингвистической экспертизы по делам о фейковых новостях.

Объяснение того, как та или иная лживая история была опровергнута, может повысить осведомленность граждан. Важно, чтобы правдивая информация была опубликована в тех же источниках с комментариями тех же авторов.

Итак, государству необходимо сохранить баланс между свободой слова и контролем за предоставленную недостоверную информацию, которая может нанести вред обществу.

Подводя итог, необходимо обозначить, что общество нуждается в разработке комплекса мер, направленных на предупреждение распространения ложных новостей и нейтрализацию последствий такого распространения.

Опасность такой информации заключается в том, что ложь может становиться оружием пропаганды. Эпидемия таких новостей ставит перед государством задачу сохранения доверия потребителей информации, все чаще отдающей предпочтение социальным сетям. Поэтому необходимо чёткое законодательное определение фейковым новостям и соответствующие меры борьбы с ними.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Собрание законодательства РФ, 04.08.2014, № 31, ст. 4398.

2. Клишин И. Максимальный ретвит: Фейк-пропаганда на новом уровне / И. Клишин // Ведомости. - 2014. - 12 февр.

3. Закон РФ от 27.12.1991 № 2124-1 (ред. от 01.03.2020) О средствах массовой информации // Российская газета, № 32, 08.02.1992.

4. ФЗ от 13.07.2015 № 264-ФЗ «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 ГПК РФ» // Российская газета, № 154, 16.07.2015.

5. Джазоян А. Е. Иллюзия «пятой власти»: как социальные сети модернизируют журналистику / А. Е. Джазоян // Ученые записки Забайкальского государственного университета. Серия: Филология, история, востоковедение. - 2014. - № 2. - С. 93-100.

6. ФЗ от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) Об информации, информационных технологиях и о защите информации // Российская газета, № 165, 29.07.2006.

7. Электронный ресурс: https://kuban.rbc.ru/

8. ФЗ от 18.03.2019 № 30-ФЗ «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» Российская газета, № 60, 20.03.2019.

9. Красовская Н.Р, Гуляев А.А, Юлина Г.Н. Фейковые новости как феномен современности // Власть. 2019. №4.

10. Электронный ресурс: https://tv.rbc.ru.

11. Суходолов А. П. «Фейковые новости» как феномен современного медиапространства: понятие, виды, назначение, меры противодействия // Вопросы теории и практики журналистики. - 2017. - Т. 6, № 2. - С. 143-169.

12. Кошкарова Н.Н. Фейковые новости: креативное решение или мошенничество? // Вестник ТГПУ. 2018. №2 (191).

ВОЗМОЖНОСТИ ГИПЕРСПЕКТРОМЕТРОВ И ПОТЕНЦИАЛ ИХ ПРИМЕНЕНИЯ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Еськов Александр Васильевич[1], alesc72@mail.ru

[1]Краснодарский университет МВД России

Аннотация. Проведено описание принципа действия современного спектрального прибора – гиперспектрометра, рассмотрены примеры применения гиперспектрометра в различных сферах деятельности человека и некоторые задачи ОВД Российской Федерации, решение которых возможно с применением гиперспектрометров.

Ключевые слова: световой спектр, техническое зрение, гиперкуб, распознавание объектов.

Приборы, которые позволяют получать спектральные изображения называются гиперспектрометрами. Изображающие гиперспектрометры обеспечат получение обширной информации о всей среде обитания на основе гиперспектрального изображения. В то время как камеры (как глаза) идентифицируют предметы по их форме или контрастам света и темноты, гипер-

спектральные сканеры могут собирать отражения на различных длинах волн ИК и автоматически определять материал, из которого сделан предмет [1].

Вместо пространственного разрешения вы получаете спектральное разрешение. Каждый материал дает коэффициент отражения в определенной полосе спектра. Гиперспектрометр собирает сотни длин волн диапазона, чтобы сформировать сигнатуру интересующего материала. Технология, разработанная для использования в космосе, теперь устанавливается на беспилотные летательные аппараты.

Изображающие гиперспектрометры имеют существенно более широкий диапазон прикладного применения, такие приборы позволяют получать высокодетальную пространственную и спектральную информацию о типе и состоянии зондируемых природных и антропогенных объектов и использовать эту информацию для решения различных задач [2].

Изображающий гиперспектрометр позволяет получить изображение, в каждой точке которого записана информация о спектральной яркости (гиперкуб). Функциональные возможности такого гиперспектрометра намного превосходят возможности обычного спектрометра. Во-первых, он позволяет получить спектр именно того объекта, который нужен оператору. Во- вторых, может быть выполнен анализ спектрального слоя гиперкуба, в котором можно будет увидеть локальные неоднородности анализируемого объекта. В качестве конкретного примера можно привести анализ растений, произрастающих на обозреваемой гиперспектрометром территории, которые в интегральном освещении (солнечный свет) выглядят однородно, но выделение некоторых спектральных слоев позволяет обнаружить отличительные особенности зон произрастания растений. В-третьих, появляется возможность объединить спектральный и текстурный анализ некоторых объектов.

Когда свет отражается от материалов, он создает особую химическую характеристику, уникальную для этого материала. Если получаемая спектральная характеристика находится в базе данных известных материалов, то один пиксель может предоставить достаточно информации для идентификации вещества. Точность часто зависит от объема библиотеки спектральных характеристик; например, военная краска на бронированном транспортном средстве может быть дифференцирована от коммерческой краски, используемой на гражданских транспортных средствах.

Ближний инфракрасный и коротковолновый инфракрасный диапазоны лучше всего различают естественную природную среду и искусственные объекты. Другое использование этих полос включает в себя поиск областей участков почвы, подверженной воздействию человеком или техникой, что поможет сканерам находить туннели и скрытые самодельные взрывные устройства по содержанию влаги в почве. При реагировании на стихийные бедствия гиперспектральные датчики могут определять, какие районы были затоплены, отслеживать распространение разлитых опасных материалов и определять место разжигания костров. Длинноволновые ИК-датчики могут использоваться для характеристики сточных вод, позволяя картографировать токсичные облака и незаконные выбросы вредных веществ в атмосферу.

Полиция может сканировать нелегальные поля наркотических растений (марихуаны, конопли, мака и т.д.), а пограничные патрули могут охотиться на контрабандные туннели через границу. В будущем скрыться от глаз будет недостаточно, чтобы оставаться скрытым от летающих роботов.

Одной из задач использования в ОВД гиперспектрометра может быть обнаружение и идентификация объектов, сбор и анализ геоинформационных данных, например, высотная съемка с использованием беспилотного летательного аппарата. Программирование маршрута следования и управление полетом может осуществляться оператором или с использованием машинного зрения. С бортового компьютера данные с геометками могут быть переданы на сервер, на котором осуществляется сбор, анализ, хранение, а также интерпретация данных, полученных с индивидуальных бортов. Анализ и сопоставление данных на сервере позволит принимать верные управленческие решения и использовать элементы прогнозирования развития ситуации.

Кроме того, разрабатываемое изделие возможно к применению и в сфере экспертизы пищевых продуктов, лекарств, стройматериалов, горюче-смазочных материалов, в качестве экспресс-метода экспертизы наркотических, взрывчатых и других запрещенных к обороту веществ и предметов, имеющих характерный оптический спектр.

Продовольственная безопасность России зависит не только от наличия продуктов питания на потребительском рынке, но и от их качества. Известно, что в настоящее время на рынке присутствует большое количество фальсифицированных продуктов питания, вино-водочных изделий, безалкогольных напитков и даже лекарств. В погоне за прибылью производители пищевых сред в процессе производства часто используют недоброкачественные и запрещенные компоненты. Технология производства, сроки и условия хранения продуктов питания часто нарушаются. Все это подрывает здоровье потребителей и даже приводит к вспышкам массовых отравлений. Почти ежемесячно в средствах массовой информации сообщается о подобных происшествиях. Особенно пагубной для населения является изготовление и реализация фальсифицированной вино-водочной продукции. «Паленая» водка вызывает тяжкие отравления, приводящие к летальным исходам.

С начала 90-х гг. прошлого века предпринимаются попытки автоматизировать тестирование пищевых продуктов, прежде всего жидких. Речь идет о разработке устройств типа «электронный язык», содержащих наборы сенсоров, подобных вкусовым рецепторам человека. Альтернативным прибором в решении задачи контроля качества продуктов питания может стать применение гиперспектрометра.

В настоящее время в России производство гиперспектрометров находится на начальном этапе, например, АНО «Кластерный инжиниринговый центр Самарской области» [2].

На мировом рынке есть множество компаний (Германия, Япония, США, Канада, Китай и др.) [3, 4], которые производят гиперспектрометры,

ряд из них заявили о разработке для использования совместно с мобильными устройствами.

Использование гиперспектрометров в деятельности ОВД можно рассматривать по конкретным задачам:

- он позволяет преодолевать любую маскировку;
- сканировать нелегальные поля наркотических растений;
- проводить экспертизу пищевых продуктов, лекарств, строительных и других материалов, исполненных чернилами документов, колориметрия;
- применяться в средствах контроля и управления доступом.

Решение приведенных задач носит принципиальный характер, а оперативность и своевременность зависит от применяемых технических средств, стоящих на вооружении современной полиции, в числе которых, на наш взгляд, могут быть использованы гиперспектрометры.

Литература

1. Fuhong Cai, Dan Wang, Min Zhu, Sailing He Pencil-like imaging spectrometer for bio-samples sensing // Biomedical Optics Express – 2017. - Vol. 8. Issue 12, P. 5427-5436.
2. Кластерный инжиниринговый центр Самарской области [Электронный ресурс]: Официальный сайт. URL:http://www.cecsr.org.
3. Технологический оптический и лазерный центр ALPhANOV, Оптический институт Аквитании, Таланс, Франция [Электронный ресурс]: Официальный сайт. URL: http://www.alphanov.com.

V.A. Blank, R.V. Skidanov Hyperspectrometcr based on a harmonic lens with diffraction grating // Journal of Physics: Conference Series. - 2017. -Vol. 1096.-P. 1-7

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В ПЕРИОД ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

Зыбин Дмитрий Георгиевич[1], zdg77@mail.ru
Калач Андрей Владимирович[1], a_kalach@mail.ru
Буркова Ксения Олеговна[1], 1998402@gmail.ru

[1]Воронежский институт ФСИН России

Аннотация. Статья посвящена выяснению отдельных аспектов обеспечения информационной безопасности и противодействию экстремизма на фоне пандемии коронавирусной инфекции COVID-19. Рассмотрены проблемы роста киберпреступности, интернет-экстремизма и возникновения нового интернет-мошенничества, названного «кибер-коронавирус». В заключение отмечены некоторые способы предотвращения утечек персональных данных сотрудников, связанные с переходом на дистанционную работу, а также меры по предотвращению распространения экстремизма.

Ключевые слова: киберпреступность, пандемия, персональные данные, утечка информации, информационная безопасность, экстремизм.

В первые месяцы 2020 года информация о возникновении новой коронавирусной инфекции, в последствии ставшей пандемией, потрясла мировое сообщество. На фоне постоянно растущего беспокойства граждан различных государств, специалисты в области информационной безопасности отметили резкое возрастание коэффициента совершаемых кибер-преступлений и интернет-мошенничества, в том числе участились случаи интернет-экстремизма [1].

В интернет-пространстве стало появляться всё больше сайтов с фальсифицированными статистическими данными о количестве подтвержденных случаев заболевания новой коронавирусной инфекцией. Специалистам по обеспечению ИБ РФ сдержать распространение ложных сведений, посредством введения поправок в УК РФ.

Сегодня за распространение заведомо ложной информации об опасных для жизни и здоровья населения обстоятельств, к которым относятся сведения о COVID-19, можно получить наказание в виде штрафа в размере от 300 тысяч рублей или в виде ограничения свободы на срок до 3 лет.

Ниже приведена официальная статистика заболеваемости стран с наиболее сложной эпидемиологической ситуацией по COVID-19 (по состоянию на 20.05.20 г. 4:00 мск) [2].

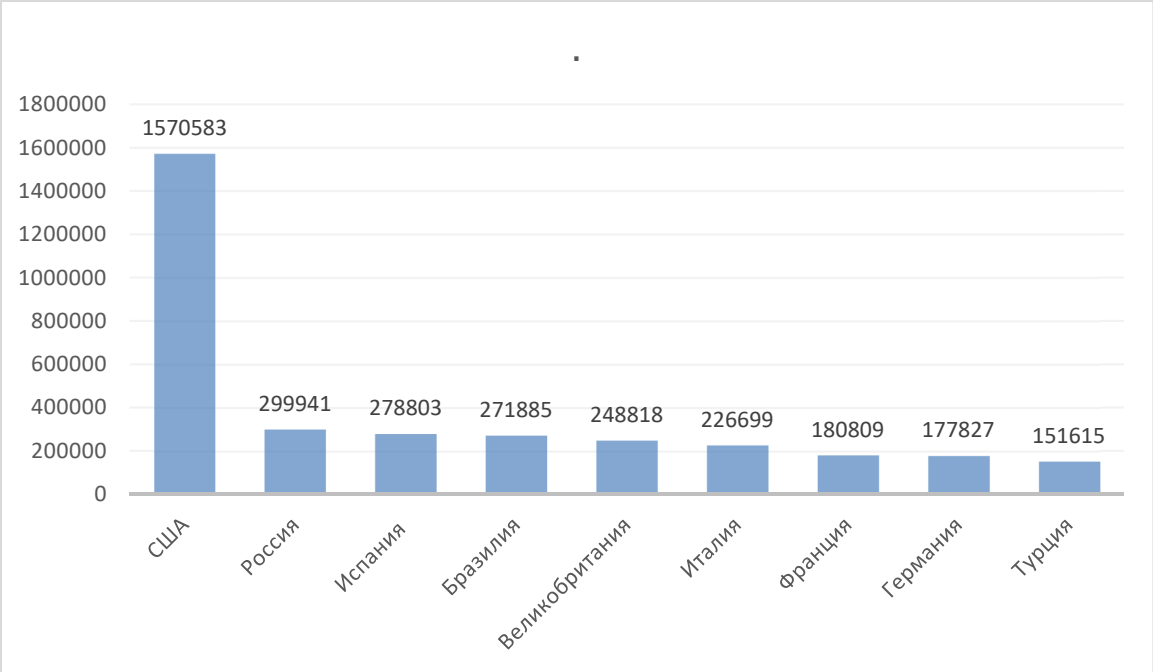


Рисунок 1. Наиболее пораженные страны (по общему количеству подтвержденных случаев)

В целях ограничения дальнейшего распространения коронавирусной инфекции COVID-19 ряд стран приняли решение о введение ограничительных мер для граждан своих стран. Согласно Указу Президента РФ от

02.04.2020 N 239 "О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19)" работодателям различных сфер деятельности было поручено перевести максимально возможное количество работников на удаленную работу. Соответствующие меры также приняло и руководство ФСИН России.

Таким образом, сегодня сотрудников УИС системы можно условно разделить на две категории: сотрудники, имеющие возможность работать дистанционно и сотрудники, отвечающие за нормальную работу учреждения, осуществляющие надзор за осужденными, подозреваемыми или обвиняемыми, без возможности перехода на удаленную работу. Особое внимание в статье уделяется первой категории сотрудников, поскольку проблема киберпреступности при работе таких сотрудников становится очень актуальной.

В настоящее время паника в интернет-пространства спровоцировала появление новой информационной угрозы «кибер-коронавируса», подвергнув риску категорию граждан, работающих дистанционно. Злоумышленники «новой интернет-угрозы» выдают себя за сотрудников Всемирной Организации Здравоохранения (ВОЗ), после чего пытаются получить персональные данные граждан. Как правило, это происходит с помощью отправки писем на электронную почту населения, в которых содержится ссылка, переходя по которой можно якобы получить секретную информацию о распространении COVID – 19. [3]

Из-за огромной утечки персональных данных в глобальной сети стали не редкими и случаи интернет-экстремизма, всё чаще в комментариях к сайтам, которые выдают «секретную информацию о больных COVID – 19» группы лиц пишут оскорбительные комментарии, призывая к уничтожению граждан больных короновирусной инфекцией. Также стало известно о направлении материалов прокуратуры Пензенской области в Генеральную прокуратуру РФ с требованием принять меры по ограничению доступа к информации, содержащей призывы к осуществлению экстремистской деятельности. Из материалов стало известно, что в ходе мониторинга одного из сообществ социальной сети «Вконтакте» пользователь разместил комментарий с высказываниями побудительного характера, призывающего к враждебным действиям по отношению к группе лиц, заболевших коронавирусной инфекцией, также автор комментария призывал к закрытию любых транспортных сообщений в области. На данный момент в отношении автора комментария решается вопрос о возбуждении уголовного дела по ч. 2 ст. 280 УК (публичные призывы к осуществлению экстремистской деятельности) [4].

Аналитический центр InfoWatch прогнозирует двукратный рост утечек персональных данных сотрудников, переведенных на удаленную работу, о чем свидетельствует четырёхкратное увеличение рассылки фишинговых сайтов. Также аналитиками были приведены некоторые примеры утечек и экстремистских действий, связанных с распространением COVID-19 [5]:

В Узбекистане распространялась информация о гражданах, заразившихся коронавирусной инфекцией и находящихся на карантине. Рабочая группа МВД выявила более 30 аккаунтов, с которых распространялась ложная информация о COVID-19

2) В Казахстане были раскрыты данные семи личностей, в том числе и детей, которые контактировали с заразившейся коронавирусной инфекцией женщиной. Персональные данные, в том числе даты рождения, места проживания, адреса регистрации и номера телефонов оказались в Wats-app – рассылке.

13 марта 2020 года университетская больница Брно в Чехии, которая проводит тесты на коронавирус, подверглась кибер-атаке. На тот момент в стране было зарегистрировано 140 случаев заражения коронавирусной инфекцией COVID-19 и 4800 человек были изолированы и находились на карантине. Из-за отключения информационных систем многие пациенты получили результаты тестов с очень большой задержкой, многих тяжелобольных пришлось перевести в ближайшую больницу

4) Случаи экстремизма были выявлены в наиболее популярных приложениях для проведения видеоконференций, примером является появление еще одной новой информационной угрозы, получившей название Zoom Bombing. В зафиксированных случаях этого явления злоумышленники намеренно проникали в наиболее уязвимые конференции с целью шпионажа или пропаганды экстремизма, также неизвестные присоединялись к онлайн-урокам известных школ - выкрикивали нецензурные слова, воспроизводили ролики порнографического содержания или же как в инциденте, который стал известен ФБР, показывают различные нацистские символики и призывают к ненависти.

Однако опасность информационной среды составляют не только киберпреступники и вредоносное ПО, также не стоит забывать о таком потенциальном нарушителе, как сотруднике учреждения.

По данным аналитического центра InfoWatch на 17 апреля 2020 г, был представлен отчет по утечкам информации с 2013 по 2019 г. В отчете авторы особое внимание уделили внутренним утечкам, так согласно источнику, за 2019 год внутренние нарушители спровоцировали 53,7% всех утечек информации, а объем скомпрометированных данных составил более 9,87 млрд записей.

Динамика последних лет свидетельствует о необходимости переосмысливания существующих требований информационной безопасности в сторону их ужесточения и необходимости особого контроля возникновения экстремизма. В целях обеспечения информационной безопасности и предотвращения дальнейшего развития экстремисткой деятельности во время пандемии, связанной с распространение COVID-19, необходимо принять следующие меры:

1. Ввести поправки в существующее законадальство РФ, относительно мер применямых по борьбе с экстремизмом, в сторону их ужесточения.

2. Повысить контроль за деятельностью сотрудников, выполняющих в учреждениях работу, связанную с противодействием экстримизма и терроризма.

3. Для сотрудников, работающих удаленно необходимо ввести требования, касаемые обязательного наличия лицензированного антивирусного продукта, произвести обязательную настройку шифрованя WI-FI, а в качестве приложений и сервисов для передачи данных использовать корпоративную почту или иные проверенные мессенджеры.

4. В целях выявления «внутреннего нарушителя» информационной безопасности рекомендуется установить дополнительные модули, позволяющие удаленно контролировать рабочие места сотрудников и получать отчеты об инцидентах.

5. Для разрешения проблем технической составляющей на удаленной работе предлагаются следующие варианты: работа сотрудников на собственных ПК, при условии, что все необходимые процессы находятся в частном облаке; также возможность удаленной работы с помощью подключения к рабочей станции посредством программ удаленного доступа (VDI), тогда сотрудник имеет возможность использовать те же приложения и сервисы, какими пользовался на своем рабочем месте; второй вариант – обеспечеие сотрудников служебными ноутбуками, с уже установленными сертификатами безопасности и необходимым ПО; третий вариант – организация удаленного доступа с помощью VPN (частной виртуальной сети).

Литература

1. Вспышка коронавирусной инфекции COVID-19 [Электронный ресурс] URL: https://www.who.int/ru/emergencies/diseases/novel-coronavirus-2019 (дата обращения: 30.03.2020)

2. Коронавирус: статистика по странам [Электронный ресурс] https://index.minfin.com.ua/reference/coronavirus/geography/ (дата обращения: 20.05.2020)

3. ESET предупреждает о действиях киберпреступников в связи с эпидемией коронавируса [Электронный ресурс] URL:https://www.esetnod32.ru/company/press/center/eset-preduprezhdaet-o-deystviyakh-kiberprestupnikov-v-svyazi-s-epidemiey-koronavirusa/ (дата обращения: 30.03.2020)

4. Генеральная прокуратура Российской Федерации потребовала ограничить доступ к информации, содержащей призывы к экстремизму [Электронный ресурс]. URL: https://genproc.gov.ru/smi/news/genproc/news-1818170/ (дата обращения: 20.05.2020).

5. Как утекает информация по Covid-19 InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/digest/24353. (дата обращения: 20.05.2020)

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА К АВТОМАТИЗИРОВАННЫМ РАБОЧИМ МЕСТАМ В УСЛОВИЯХ КРИТИЧЕСКОЙ СИТУАЦИИ

Иванова Мария Евгеньевна[1], maryy-4225522@yandex.ru
Душкин Александр Викторович[1,2,3], a_dushkin@mail.ru

[1]Национальный исследовательский университет
«Московский институт электронной техники»
[2]Военный учебно-научный центр Военно-воздушных сил
«Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»
[3]Воронежский государственный технический университет

Аннотация. В настоящей работе предложена методика автоматизированной настройки защищенного удаленного доступа к рабочим местам через межсетевой экран. Программное обеспечение, разработанное в ходе исследования, добавляет любое количество пользователей в глобальную политику безопасности, что позволяет значительно уменьшить временные затраты. Это особенно актуально в условиях критической ситуации и ограниченных сроков. Такой метод позволяет в кратчайшие сроки организовать доступ к рабочим местам с мобильных устройств сотрудников.

Ключевые слова: администратор, защита информации, информационная безопасность, межсетевой экран, удаленный доступ

Актуальной задачей такого направления информационных телекоммуникационных технологий, как информационная безопасность, является защита сведений конфиденциального характера. Одним из самых популярных средств для защиты локальной вычислительной сети организации является межсетевой экран, выполняющий фильтрацию сетевых потоков согласно заданным администратором безопасности правилам.

Количество пользователей корпоративной сети может широко варьироваться. Тем не менее, по каждому из них необходимо добавить правила фильтрации, которые определяют права доступа пользователя к тому или иному ресурсу. Ручное прописывание матрицы доступа в консоль управления межсетевым экраном может привести к опечаткам и большим временным затратам. Таким образом, если правила фильтрации формируются по определенному шаблону, выгодно автоматизировать данный процесс. Например, для организации удаленного доступа сотрудников к рабочим местам необходимо прописать следующие параметры в центр управления политиками: IP-адрес автоматизированного рабочего места пользователя, персональный сертификат пользователя и доверенный удостоверяющий центр, создать пользователя с соответствующими фамилией, именем и отчеством. По описанным входным данным можно создать шаблон, с помощью которого процедура перевода сотрудников на удаленную работу станет тривиальной процедурой.

Для решения поставленной задачи разработана программа для межсетевого экрана, написанная на языке программирования C++, совместимая с сервисом REST API Центра управления политиками. С помощью нее возможно вносить данные пользователей в текущую глобальную политику безопасности организации без дополнительных настроек.

При создании шаблона для перевода на удаленную работу должны быть проанализированы следующие нюансы организации безопасного подключения.

Во-первых, для построения правил фильтрации необходимо учитывать общую глобальную политику безопасности организации. Есть два типа наборов правил: «пропускать» и «запрещать». Если изначально для всех объектов топологии сети выставлена политика «Пропускать всё», то правила прописываются на запрет определенного трафика. Если изначально – «Запрещать всё», то правила прописываются на разрешение приема и передачи заданного трафика. Второй способ является наиболее безопасным, так как исключает пропуск вредоносного трафика, который не был учтен при построении правил пропуска информационных потоков.

Во-вторых, необходимо обеспечить идентификацию и аутентификацию пользователей, которому предоставляются разрешенные сервисы. Это исключает доступ посторонних лиц к рабочему компьютеру. Персональным идентификатором пользователя могут являться пароли, сертификаты и токены. Выпускать персональные сертификаты можно с помощью Удостоверяющего центра на базе служб сертификации Active Directory. Чтобы снять нагрузку с администратора безопасности и автоматизировать процесс генерации сертификатов, следует использовать распределенный способ генерации персональных сертификатов и контейнеров закрытого ключа. В разработанной программе предусмотрен автоматизированный выпуск сертификатов по запросам от пользователей. При этом контейнер закрытого ключа создается прямо на личном компьютере сотрудника и не передается администратору безопасности.

В-третьих, журналирование событий должно происходить при любом действии пользователя для того, чтобы в случае возникновения инцидента была возможность восстановить достоверную картину.

Управление межсетевым экраном осуществляется с помощью Центра управления политиками, который имеет графический интерфейс. Обычно он располагается на отдельном устройстве и обеспечивает добавление, просмотр, редактирование и удаление правил фильтрации.

На операционных системах семейства Windows поддерживается подключение к удаленному рабочему столу с помощью стандартных средств по протоколу RDP, использующий порт 3389 по умолчанию. Чтобы подключиться к удаленному компьютеру достаточно ввести его IP-адрес и учетные данные пользователя.

Для маскировки компьютеров, расположенных в корпоративной сети организации, применяется технология NAT. Настоящие IP-адреса скрыты за

IP-адресом внешнего интерфейса маршрутизатора или межсетевого экрана, на котором прописаны маршруты до компьютеров сети.

Для того, чтобы ограничить действия пользователя в локальной вычислительной сети, следует предоставить конкретному сотруднику доступ только к своему рабочему месту и запрещать все остальные информационные потоки.

Рассмотрим пример корпоративной сети, рассчитанной на 3000 пользователей, которым необходимо обеспечить удаленный доступ к рабочим компьютерам из дома. В данной сети уже существуют ранее созданные правила фильтрации между автоматизированными рабочими местами, не влияющие на формирование новых. Они функционируют в пределах границы контролируемой зоны организации и обеспечивают доступ ко всем необходимым ресурсам. Такие условия доступа должны остаться после внесения изменений в глобальную политику безопасности. Редактирование настроек на центре управления политиками, которые одинаковы для каждого из пользователей, может быть рутинной и долгой задачей, так как в интерфейс управления межсетевым экраном необходимо добавить следующие сведения:

− пользователей, в роли которых выступают домашние персональные компьютеры;

− персональные сертификаты, необходимые для авторизации пользователей в сети;

− АРМ, для которых будет прописан реальный IP-адрес;

− правила доступа для пользователей к своим АРМ.

В качестве входных данных программы выступает таблица пользователей в формате CSV UTF-8 (разделитель – запятая). В таблице представлен пример данных, сохраненных в файл data.csv (см. Таблица 1).

Таблица 1 – Входные данные пользователей

ФИО	**Сертификат**	**IP-адрес АРМ**
Сидоров Иван Петрович	CN=Сидоров Иван Петрович,C=RU	10.111.1.113
Петров Петр Иванович	CN=Петров Петр Иванович,C=RU	10.111.1.114
Орлова Ольга Юрьевна	CN=Орлова Ольга Юрьевна,C=RU	10.111.1.117

С помощью программы в автоматическом режиме новые настройки записываются со скоростью 3000 пользователей за 10 минут. Ручное добавление пользователей занимает несколько дней.

Центр управления политиками содержит дополнительный интерфейс взаимодействия с пользователем – REST API, использующий протокол HTTP и формат представления данных XML. С помощью него возможно получать

данные из базы данных, создавать новые объекты, редактировать данные и автоматизировать процессы.

В состав разработанного программного обеспечения входят следующие компоненты:

конфигурационный файл добавления пользователя, сертификата, автоматизированного рабочего места и правила в формате XML;

исполняемый файл программы;

программа командной строки curl.exe, дающая возможность взаимодействовать WEB-интерфейсом REST API;

входные данные о пользователях;

файл журналирования действий программы.

Программа автоматизации выполняет следующую последовательность действий:

− ввод учетных данных администратора безопасности;

− создание сессии временного доступа к функционалу центра управления политиками;

− считывание входных данных (см. Таблица 1);

− создание конфигурационного XML-файла;

− создание сессионного токена для доступа к интерфейсу REST API;

− загрузка конфигурационного XML-файла в WEB-обозреватель;

генерация персонального сертификата;

− логирование результата операции (см. Рисунок 1);

− удаление токена и XML-файла;

− вывод информации о количестве добавленных пользователей.

Программа исполняется, пока не добавит всех прописанных сотрудников.

В исходную топологию локальной сети добавятся следующие объекты:

− 3000 АРМ;

− 3000 пользователей;

− 3000 правил фильтрации;

− 3000 персональных сертификатов пользователей.

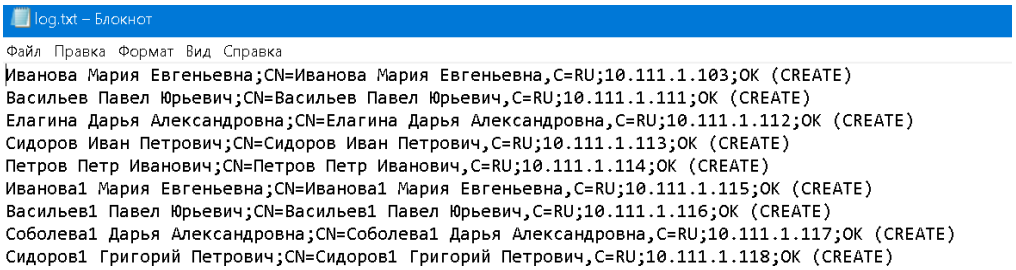


Рисунок 1 – Логирование

Для того, чтобы проверить работоспособность новых настроек межсетевого экрана необходимо создать виртуальный стенд, который состоит из центра управления политиками, межсетевого экрана, рабочего компьютера сотрудника и его домашнего компьютера. На домашнем компьютере открыть «Подключение к удаленному рабочему столу», вписать IP-адрес удаленного

рабочего стола и учетные данные пользователя. В результате подключение выполняется успешно (см. Рисунок 2).

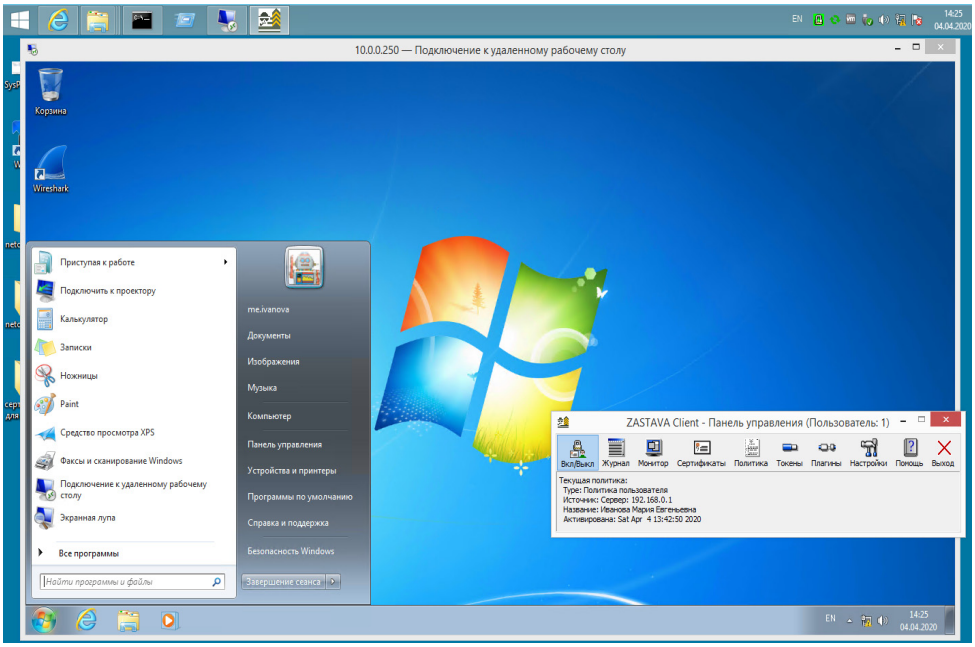


Рисунок 2 – Удаленный рабочий стол АРМ

В настоящей статье рассмотрена методика автоматизированной настройки защищенного удаленного доступа к рабочим местам через межсетевой экран. Разработанное программное обеспечение автоматизирует процесс добавления пользователей, их персональных идентификаторов и правил фильтрации в Центр управления политиками межсетевого экрана. Такой метод позволяет сократить временные затраты в несколько сотен раз и в кратчайшие сроки организовать доступ к рабочим местам с мобильных устройств сотрудников. Это особенно актуально в условиях критической ситуации и ограниченных сроков.

Литература

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб.: Питер, 2019. 992 с.

2. ГОСТ Р ИСО/МЭК 27033-1–2011. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции // Национальный стандарт Российской Федерации. М.: Стандартинформ, 2012. 135 с.

3. http://www.fstec.ru/ – сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

4. Scarfone K., Hoffman P. Guidelines on Firewalls and Firewall Policy Karen Scarfone Paul Hoffman: Recommendations of the National Institute of Standards and Technology. Revision 1. U.S.: NIST Special Publication 800-41, 2009. p.p. 48.

5. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности. М.: Горячая линия – Телеком, 2016. 248 с. ISBN 978-5-9912-0470-5.

6. Я.Г., Душкин А.В., Кравченко А.С., Панычев С.Н., Сахаров С.Л. Некоторые прикладные вопросы информационной безопасности систем обработки информации. Современные наукоемкие технологии. 2016. №8-1. С. 41-45.

ЛИНГВИСТИЧЕСКАЯ ДИАГНОСТИКА СЛОВЕСНОГО ЭКСТРЕМИЗМА

Колесникова Ирина Евгеньевна[1], Irak07@mail.ru

[1]Крымский филиал Краснодарского университета МВД России

Аннотация. В статье рассматриваются особенности параметризации словесного экстремизма с учетом лингвистических и юридических знаний. Это исследование требует использование понятия призыва как речевого акта в контексте юридических реалий.

Ключевые слова: экстремизм, речевой акт, призыв, контекст, судебно-лингвистическая экспертиза.

Выявление словесного экстремизма в публичной коммуникации диктует привлечение специальных лингвистических знаний, которые используются при решении юридических вопросов.

Слово, написанное или сказанное в определенных обстоятельствах, предусматривает юридические последствия.

Поэтому судебно-лингвистическая экспертиза заявила о себе как об относительно новой отрасли науки, имеющей межпредметный характер. Учитывая современные реалии, следует отметить одно из актуальных заданий разработки процедуры диагностики речевых актов на предмет наличия или отсутствия «экстремистских» маркеров.

Объектом статьи стали «продукты речевой деятельности» [3, С. 4], зафиксированные в текстовой или аудиовизуальной форме на «материальном носителе» и исследуемые на наличие или отсутствие признаков экстремизма, угроз, клеветы оскорблений [7, С. 17].

Предмет – наличие в определенном речевом или языковом уровне (или срезе) формальных признаков, соотносимые с когнитивными моделями юриспруденции.

В данном случае следует понимать текст широко: как устной форме, так и в письменной; как отдельное, так и оформленное высказывание.

На исследование могут быть представлены зафиксированные на любых носителях письменные тексты и записи устных выступлений, видео- и кинофильмы, книги, листовки и др., – то есть всё, что фиксирует результаты словесной коммуникации [8, С. 20].

Теоретическую основу работы составили труды ученых в области судебно-лингвистический экспертизы (работы Л.В. Ажнюк [1], А.Н. Баранова [2], К.И. Бринева [3], В.Ю. Меликяна [5] и др.).

По мнению А. Вежбицкой, категорию призыва следует рассматривать с помощью теории речевых актов, поскольку призыв выражает определенное коммуникативное намерение говорящего [4].

Поэтому не случайно А.Н. Баранов определяет все виды призыва (лозунга, апелляции, обращения, воззвания) как побуждение к определенным действиям [5, С. 284-285]. А сам речевой акт - это часть общественно-политической коммуникации [2, с. 420].

Рассмотрим базовые подходы при проверке текста в делах наличие словесного экстремизма.

Ситуация употребления и общий контекст. Как правило, речевой акт реализовывается в политическом дискурсе.

Грамматическое оформление. Обычно в спорном тексте присутствует призыв (прямой или косвенный), в котором и следует установить семантические маркировки побуждения к осуществлению экстремистской деятельности.

Соотношение содержания с диспозицией юридической нормы. В данном случае эксперт соотносит семантические эталоны (например, гиперидентичности) с юридическими нормами и определениями. Например, некоторые понятия имеют юридические определения и используются в своем терминологическом, а не общеупотребительном значении.

В контексте прикладной значимости следует отметить важность «технологической доступности» результатов исследования судебно-лингвистической экспертизе. Ведь результаты этих исследований применяются в сфере юриспруденции, когда толкование лингвистических реалий предусматривает юридические последствия.

Однако единой методики все же не существует. Как не существует цельного научно-методического и терминологического аппарата, адекватной подготовки специалистов. Поэтому на повестке дня стоит проведение совместных научных мероприятий, семинаров, конференций с участием представителей экспертных учреждений и профильных вузов для усовершенствования методологии и выработке стратегий в судебно-лингвистической экспертизе вообще.

Литература

1. Ажнюк Л.В. Словесний екстремізм та його лінгвістична діагностика// Одеський лінгвістичний вісник: Сецвипуск – Одеса, 2017. – С. 7-14.

Баранов А.Н. Лингвистическая экспертиза текста: теория и практика: учеб. пособие. - М.: Флинта: Наука, 2007. - 592 с.

Бринев К.И. Теоретическая лингвистика и судебная лингвистическая экспертиза: монография. – Барнаул: АлтГПА, 2009. – 252 с.

Вежбицкая А. Речевые жанры [в свете теории элементарных смысловых единиц] // Антология речевых жанров: повседневная коммуникация. – М. – 2007. – С. 68–80.

Колесникова И.Е. // Особенности призыва в судебно-лингвистической экспертизе текста. Сборник трудов научно-практической конференции для студентов и молодых ученых. – Симферополь, 2019. Изд-во Издательство: Общество с ограниченной ответственностью «Издательство Типография «Ариал»(Симферополь),- С. 284-285.

Меликян В.Ю. Типовые вопросы к эксперту-лингвисту и пределы компетенции лингвистики и права // Язык и право: актуальные проблемы взаимодействия. Материалы II-ой Международной научно-практической конференции / Отв. ред. В.Ю. Меликян. – Вып. 2. – Ростов/н/Д: Дониздат, 2012. – С. 50–58.

Подкатилина М.Л. Судебная лингвистическая экспертиза по делам об оскорблении // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – С. 389–394.

Теоретические и методические основы психолого-лингвистической экспертизы текстов по делам, связанным с противодействием экстремизму: методическое издание М-во юстиции Российской Федерации, Гос. учреждение Российский федеральный центр судебной экспертизы при М-ве юстиции Российской Федерации. – Издательство: ЭКОМ Паблишерз, 2011. - 326 с.

СПОСОБ ОРГАНИЗАЦИИ СЕТИ СВЯЗИ С ПРИМЕНЕНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Лукьянов Александр Сергеевич[1], las92@yandex.ru
Толстых Денис Сергеевич[1], tds_84@mail.ru
Штепа Сергей Дмитриевич[1], k.zero48@mail.ru

[1]Воронежский институт МВД России

Аннотация. Проведен анализ особенностей, элементов и структуры беспилотных летательных аппаратов и варианты их применения в организации мобильных сетей связи.

Ключевые слова: беспилотный летательный аппарат, радиосвязь, ретранслятор, органы внутренних дел, питание, антенна, дрон, базовая станция.

На сегодняшний день технологии сделали большой скачок в сфере радиосвязи, появилось много новых технологий и стандартов. Радиосвязь занимает важнейшее место в органах внутренних дел (ОВД), т.к. обеспечивает подразделения защищённой мобильной связью для передачи различной служебной информации. А внедрение беспилотных летательных аппаратов (БПЛА) в ОВД решило бы многие задачи по охране общественного прядка, проведению массовых мероприятий, обеспечению безопасности дорожного движения, по охране особо важных объектов, что обеспечит лучший контроль полицией и позволит быстрее выявлять правонарушителей и зачинщиков беспорядков и т.д. Уже было придумано множество концептов использования БПЛА в ОВД. Например, дроны ГИБДД, способные фиксировать нарушения ПДД, делать автоматические снимки и что самое главное они узаконены, всё что нужно сделать это лишь проверить сертификат оборудования.

БПЛА являются общим названием большой группы устройств, имеющих схожие конструктивные особенности и функции. Они подразделяются на несколько групп, по назначению: профессиональные, любительские (гоночные), военные [4]. В зависимости от той или иной группы, варьируются

технологии и оборудование применяемое при создании дрона, от материалов корпуса и до используемых технологии связи с оператором.

Основной идеей концепта – способ организации сети связи и создание БПЛА, который будет предназначен не просто для совершения полётных миссий, но и для ретрансляции сигнала, к примеру, DMR радиостанций. Для работы данного БПЛА потребуется дополнительное питание. Идея привязного (дополнительного) питания заключается в том, что дрон с оборудованием на борту поднимается на определённую высоту и для питания всех систем к нему будет подключён комбинированный кабель, который запитывает БПЛА и передаёт информацию одновременно, т.е. БПЛА будет выполнять функцию мобильной антенной вышки повышенной эффективности, за счёт того, что он почти не ограничен в высоте подъёма антенны. Уверенная связь может поддерживаться только при одновременном увеличении высоты с расстоянием, чтобы сохранялась прямая видимость между БС и БПЛА. Двигатели БПЛА не будут подвержены перегреву, т.к. они созданы на бесколлекторной основе, что не вызывает перегрева двигателей. Для осуществления привязного питания можно использовать как топливный генератор, так и внешние аккумуляторы.

В первом варианте беспилотник может быть отключен от привязного питания, если нам необходимо обеспечить оперативную ретрансляцию сигнала там, где нет возможности установить ретрансляторное оборудование. Таким образом на БПЛА устанавливаются пара источников питания, один из которых питает основные системы беспилотника, а второй питает, заранее настроенное на нужные полосы частот и каналы, ретрансляторное оборудование. Минус такого варианта является его экономическая не выгодность, т.к. на сам БПЛА будет установлен дорогостоящий малогабаритный DMR-ретранслятор (РТР). А при наличии модульности, можно заменить ретранслятор DMR, к примеру, на камеру с высокой разрешающей способностью и модуль WiMAX, по которому можно как передавать видео сигнал, так и передавать сигналы управления, с чем данная технология вполне может справится. Таким образом БПЛА превращается в летающую камеру, способную как вести разведку, так и видео документацию каких-либо событий.

Второй вариант привязывает БПЛА к одной точке, и не даёт от неё отвязаться, т.к. без подключенного к антенне наземного РТР передача информации происходить не будет. Зато этот вариант экономически доступнее, так как тяжёлые DMR ретрансляторы имеют как меньшую стоимость, так и более высокие показатели характеристик. Теперь для упорядочивания информации рассмотрим две схемы, для первого и второго варианта. Для начала определимся, что необходимо для создания простого БПЛА, в функционал которого будет входить набор определённой высоты и полёт с ограниченной скоростью и возможностью передачи полезной нагрузки на БС [1]. Состав основной системы: полётный контроллер, реле питания, приём-

ник\передатчик, бесколлекторные двигатели беспилотника, корпус, встроенные аккумуляторы.

На рисунке 1 изображена схема простейшего БПЛА типа «квадрокоптер» которая включает в себя основные части: 1. Место для установки полётного контроллера и его модулей. 2. Реле питания, т.е. основное и дополнительные контроллеры оборотов двигателей. 3. Встроенные, извлекаемые источники питания. Как говорилось ранее, один для питания основных систем, а второй для устанавливаемого на второй ярус корпуса модуль. 4. Пропеллеры, отвечающие за создание тяги, совместно с двигателями. 5. Приёмник\передатчик для управления БПЛА и получения от него телеметрической информации и простейшие антенны с круговой диаграммой направленности (штыревые).

Таким образом получаем беспилотник способный к полёту в пределах прямой видимости. А для того, чтобы управлять БПЛА за пределами видимости человеческого зрения необходима установка как минимум аналогового ТВ передатчика и курсовой FPV камеры [3].

Рассматривая первый вариант (рисунок 2 и рисунок 3), в данную схему необходимо добавить на второй ярус корпуса, который располагается на плоскости выше места расположения основных систем, дополнительный модуль, например, малогабаритный ретранслятор DMR и запитать его дополнительным элементом питания, если нам необходим мобильный PTP. Если же есть необходимость провести видеосъёмку какого-либо места, тогда заменяем PTP на камеру и модем WiMAX (не исключено использование и мобильного LTE модема заместо WiMAX). Всё вместе, к сожалению, установить на такую платформу не получится, т.к. возрастёт общая масса БПЛА. Это можно решить увеличением тяги, сделав из него «гексакоптер» или «окатакоптер», но тогда ему потребуются более емкие аккумуляторы и более мощное реле питания, т.е. можно реализовать мобильный вариант БПЛА.

На данной схеме (рисунок 2) видно, что на БПЛА с верхней стороны был установлен второй ярус, на котором закреплён ретранслятор DMR (1) и его антенна (2). Сам ретранслятор соединён со вторым источником питания, не зависящим от первого, специально для питания дополнительного модуля.

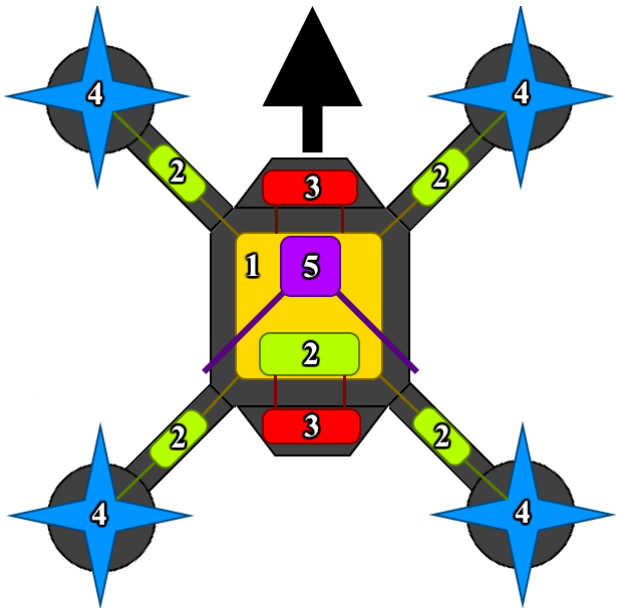


Рисунок 1. Основная структура БПЛА типа «квадрокоптер»

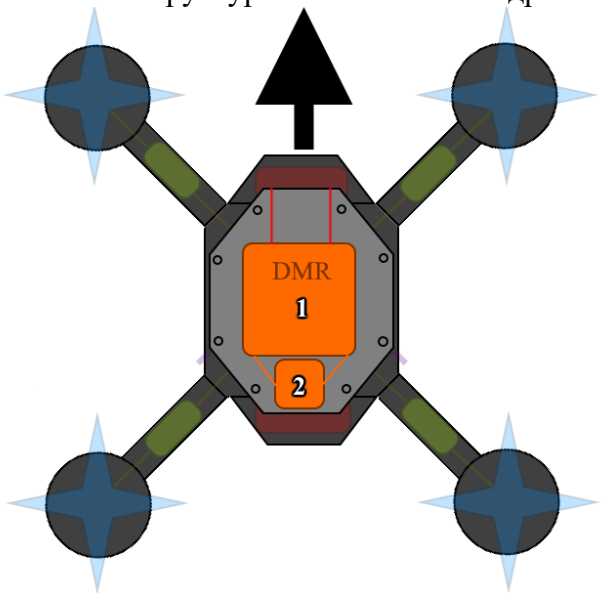


Рисунок 2. БПЛА с установленным DMR ретранслятором и антенной

При использовании ретранслятора, установленного на БПЛА, появляется возможность обеспечивать связью на определённом участке местности, но на не большое время, около 15 минут. Управление БПЛА может осуществляться прямиком из патрульного автомобиля по аналоговому каналу связи с пульта управления, а также, если срочно нужно установить связь с группой расположенной за пределами зоны покрытия радиостанции.

А для того, чтобы не потерять беспилотник в случае разряда аккумулятора можно заранее запрограммировать аварийные GPS метки, куда беспилотник автоматически направится. Например, на ближайший пост ГИБДД или отдел полиции. Схема работы данного варианта использования будет выглядеть следующим образом (рисунок 3):

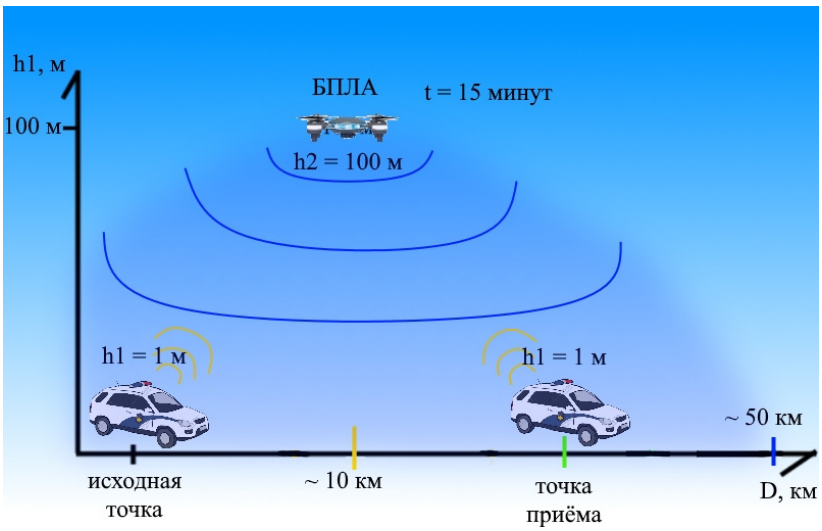


Рисунок 3. Схема применения варианта с установленным малогабаритным ретранслятором DMR

На данной схеме (рисунок 4) видно, что на БПЛА был установлен второй ярус, но с нижней стороны, для того чтобы камера (2) могла охватить то, что находится под висящим в воздухе дроном. На этой же плоскости располагается и WiMAX модем (1) со встроенной или подключаемой дополнительно антенной. В данном случае если появляется необходимость срочно узнать обстоятельства происходящего, можно установить модуль WiMAX с камерой, соединить его с БС и отправить на место происшествия. Это будет значительно быстрее, чем отправить туда патрульный автомобиль (если он не находится в непосредственной близости), потому что скорость беспилотника может достигать примерно 100 км/ч и по прямой траектории, без препятствий.

Со вторым вариантом (рисунок 5) всё немного проще, в схеме будет второй ярус, как и на первом варианте, но он будет необходим только для установки на него антенны от наземного РТР. Также понадобится комплект из кабеля и коннекторов для подключения привязного питания и антенны РТР к БПЛА и источник питания в виде бензинового генератора с преобразователем напряжения. Еще для управления дроном также используются антенны, которые нужно «изолировать» от антенны РТР, чтобы не было взаимных помех.

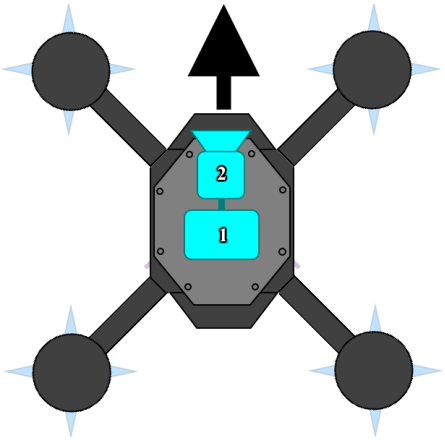


Рисунок 4. БПЛА с установленным программируемым WiMAX модемом и камерой

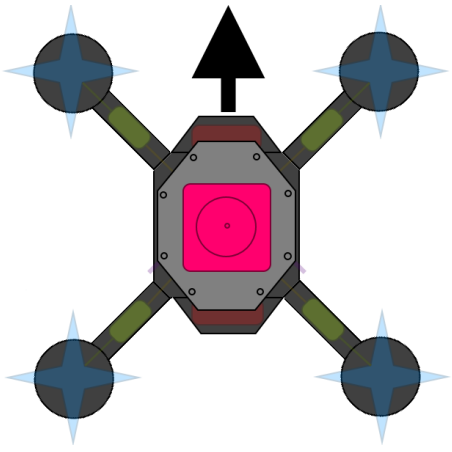


Рисунок 5. БПЛА с установленной на втором ярусе антенной наземного РТР и привязным питанием

Схема работы данного варианта использования будет выглядеть следующим образом (рисунок 6):

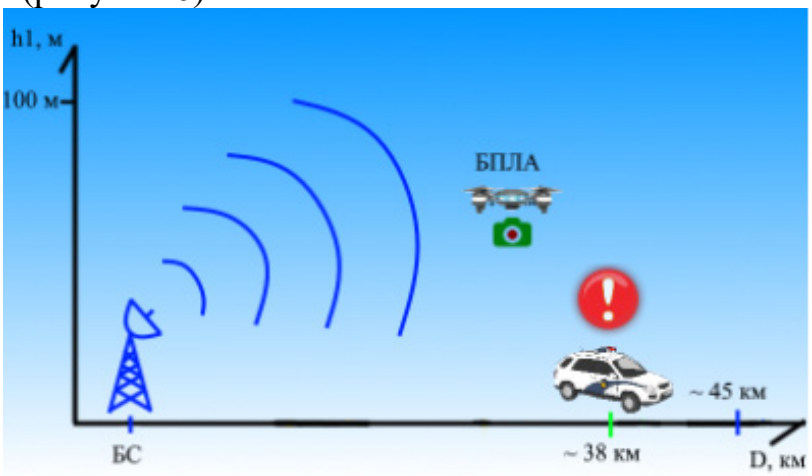


Рисунок 6. Схема применения варианта с использованием WiMAX камеры

В итоге это позволит БПЛА подняться на высоту, ограниченную длиной и весом кабеля и обеспечивать связью достаточно большую площадь на время, ограниченное лишь запасом энергии батарей или топлива генератора, и ресурсом двигателей, но у этого варианта не будет такой мобильности как у первого. Схема работы данного варианта использования будет выглядеть следующим образом (рисунок 7):

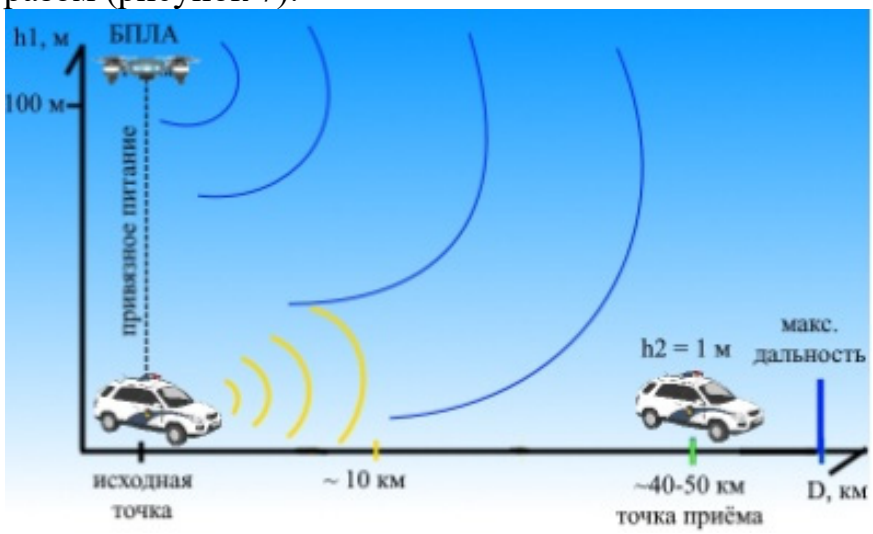


Рисунок 7. Схема применения варианта с привязным питанием

В данном случае можно увидеть, на сколько выше эффективность БПЛА по сравнению с мобильной радиостанцией. За счёт более высокой высоты подъёма можно обеспечивать связь на значительно большее расстояния. Единственное ограничение данного способа – неподвижность всей системы. Конечно, можно программными методами заставить БПЛА двигаться за автомобилем не теряя контакт с привязным питанием, но это очень сложно. Автомобиль двигается с непостоянной скоростью, может постоянно перестраиваться из ряда в ряд, совершать повороты. Беспилотнику будет трудно сохранять соединение с автомобилем.

Исходя из анализа и приведённых предложений можно отметить, что использование в ОВД данных технологий вполне обоснованно, и чтобы осуществить идеи в жизнь необходимо проводить дополнительные исследования в этом направлении. БПЛА имеют довольно широкий спектр назначений, из-за чего они могут иметь самую разную конструкцию и оснащение. А с использованием ретрансляторов WiMAX можно добиться достаточно большой дистанции связи с БПЛА.

Мобилизация устройств связи на данный момент очень востребована, разрабатываются всё более новые и сложные технологии связи, а сами устройства становятся более интеллектуальными и быстрыми в повседневных задачах. Конечно, сами государственные органы не могут заниматься разработкой и производством на прямую, поэтому эта задача должна ложится на специализированные организации, с которыми бывает ряд разногласий.

Тем не менее все варианты могли бы использоваться в системе ОВД для обеспечения быстро развёртываемой оперативной связи с повышенной эффективностью за счёт использования преимуществ БПЛА.

Литература

1. Бецков А. В. Предложения по формированию концепции применения и развития робототехнических комплексов в МВД России // Труды международного симпозиума надежность и качество. 2016. № 1. с. 62–66.

2. Василин, Н.Я. Беспилотные летательные аппараты / Н.Я. Василин. – М.: Попурри, **2012.** – 272 с.

3. Грачев Ю. А. Современные роботизированные системы, применяемые в органах внутренних дел // Ю. А. Грачев, А. А. Кежов // Судебная экспертиза: прошлое, настоящее и взгляд в будущее: материалы всерос. науч.-практ. конф. СПб.: Санкт-Петербург. университет МВД России, 2016. С. 97–100.

4. Лукьянов А. С. Перспективы развития беспилотных летательных аппаратов и их использование в ведомственных структурах / А. С. Лукьянов, С. Д. Штепа // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций: Воронежский филиал ФГБУ ВО Ивановской ПСА ГПС МЧС РФ: сб. науч. тр. – Воронеж, 2018. – С. 406-410.

5. Лукьянов А. С. Перспективы развития беспилотных летательных аппаратов и их использование в ведомственных структурах / А. С. Лукьянов, С. Д. Штепа // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций: Воронежский филиал ФГБУ ВО Ивановской ПСА ГПС МЧС РФ: сб. науч. тр. – Воронеж, 2018. – С. 406-410.

МЕТОДИКА ВЫЯВЛЕНИЯ ФАКТОВ ФИНАНСИРОВАНИЯ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Макуха Максим Юрьевич[1], mmkrdu@yandex.ru
Клюев Станислав Геннадьевич[2], s.g.klyuev@mail.ru

[1]Краснодарский университет МВД России
[2]Краснодарское высшее военное училище

Аннотация. В статье приведены наиболее распространенные источники и способы финансирования экстремистской и террористической деятельности. Определена актуальность использования криптовалют для финансирования данной деятельности. Представлен перечень мероприятий необходимых для выявления лиц участвующих в финансировании экстремистской и террористической деятельности с применением криптовалют. Описан способ наблюдения за транзакциями, интересующего Bitcoin-адреса.

Ключевые слова: экстремизм, терроризм, Bitcoin, криптовалюта, Bitcoin-кошелек, Bitcoin-адрес, Bitcoin-миксер, пылевая атака.

Согласно состоянию преступности в Российской Федерации за январь-март 2020 года зарегистрировано преступлений экстремистской направленности и террористического характера 210 и 548 соответственно, что превышает показатели аналогичного отчетного периода прошлого года на 40,9 % касаемо преступлений экстремистской направленности и 13,7 % террористического характера [1].

В части 1 статьи 1 Федерального закона «О противодействии экстремистской деятельности» [2] дано понятие экстремистской деятельности (экстремизму). Финансирование деяний в представленном перечне относится к экстремистской деятельности (экстремизму).

Существование любого рода деятельности без финансирования не представляется возможным, что также относится к экстремистской и террористической деятельности.

Среди отечественных ученых, рассматривающих вопросы финансирования экстремистской и террористической деятельности в своих работах, являются: Е.В. Каймак (актуальные вопросы выявления финансирования экстремистской деятельности и терроризма) [3]; В.Б. Батоев, В.В. Семенчук (использование криптовалюты в преступной деятельности: проблемы противодействия) [4]; П.И. Иванов (оперативно-розыскное сопровождение противодействия финансированию экстремистской деятельности: основные проблемы и пути решения) [5]; Р.Р. Абдулганеев (предупреждение финансирования деятельности религиозной экстремистской организации) [6] и другие.

К наиболее распространенным источникам финансирования экстремистской и террористической деятельности можно отнести следующие:

получение средств законными способами;

привлечение средств в сети интернет;

получение средств незаконными способами (доходы от криминальной деятельности членов преступных организаций и финансирование от экстремистских и террористических групп, находящимися за пределами России).

Наиболее распространенные источники финансирования экстремистской и террористической деятельности представлены на Рисунке 1.

Рисунок 1. Источники финансирования экстремистской и террористической деятельности.

Также важным фактором в финансировании экстремистской и террористической деятельности являются способы перемещения средств, к которым можно отнести:

использование наличных;

денежные переводы с использованием банковских счетов и банковских карт;

денежные переводы без открытия банковских счетов;

использование криптовалют.

Использование криптовалют в целях финансирования экстремистской и террористической деятельности является актуальным в связи с относительной анонимностью, а также невозможностью блокирования или ареста криптокошелька.

По данным аналитического сервиса CoinMarketCap [7] наиболее популярными криптовалютами с высоким курсом и уровнем капитализации являются: Bitcoin, Ethereum, XRP, Tether, Bitcoin Cash, Bitcoin SV и другие.

В данном контексте будет рассматриваться Bitcoin ввиду его высокого уровня популярности и уровня капитализации.

Для выявления фактов финансирования экстремистской и террористической деятельности с использованием криптовалют и установлении лиц, совершающих данные транзакции ряд действий называемых «Пылевая атака».

Суть данного метода заключается в том, что все Bitcoin транзакции в blockchain доступны для просмотра любому желающему. В случае установления личности и связи ее с определенным Bitcoin адресом появляется возможность отследить все операции совершенные этим лицом. Однако современные Bitcoin кошельки обладают возможностью создавать большое количество различных Bitcoin адресов.

Сумма, находящаяся на счете Bitcoin кошелька, состоит из UTXO (unspent transaction output) — выход неизрасходованных транзакций, которую

пользователь получает и может израсходовать в бедующем. Каждый адрес кошелька обладает собственным UTXO и связать эти адреса между собой является задачей субъекта, проводящего «пылевую атаку».

Для установления связи между адресами необходимо перевести на один из известных адресов «пыль» – 100-200 сатоши, что образует UTXO и даст возможность наблюдать за последующими транзакциями данного адреса. В случае отправления транзакции с кошелька, в отношении которого была применена «пылевая атака», превышающую каждый из UTXO, будет сформирована транзакция из UTXO разных адресов, принадлежащих кошельку, в том числе и UTXO образованное в результате «пылевой атаки», что позволит определить перечень адресов принадлежащих одному кошельку так как в данной транзакции присутствовал не потраченный выход сформированный в результате «пылевой атаки». После необходимо проверить каждый выявленный адрес на предмет нахождения информации о владельце в открытом доступе.

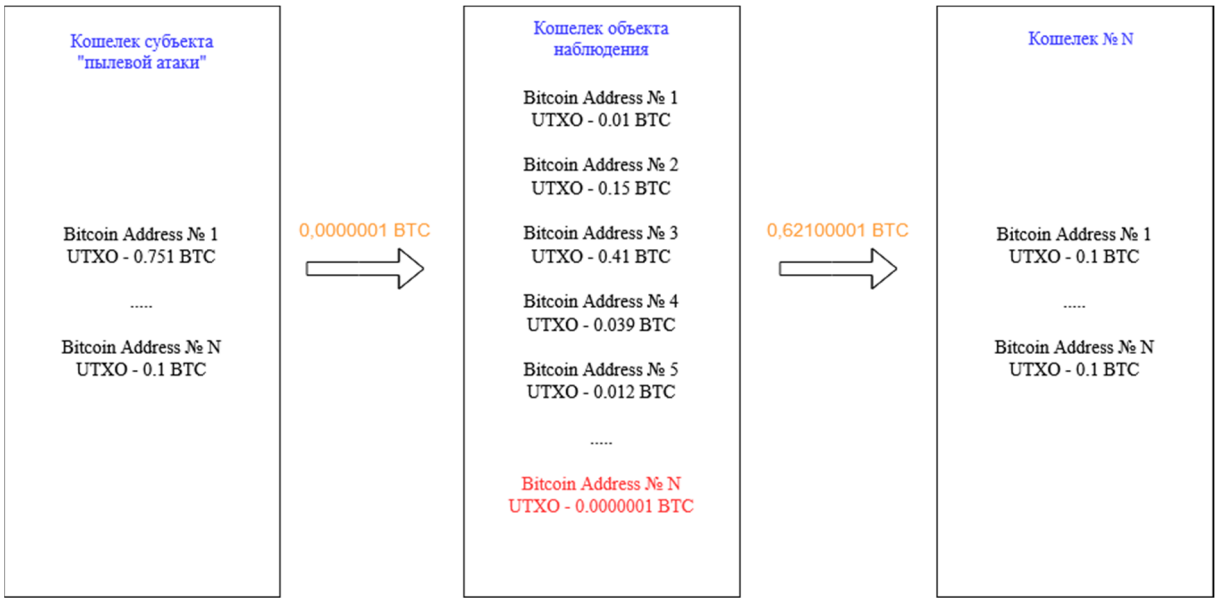


Рисунок 2. Реализация «пылевой атаки».

Для эффективного выявления фактов финансирования экстремистской и террористической деятельности с использованием криптовалют в дополнении к вышеописанному методу необходимо сотрудничество с криптовалютными биржами, обменниками и Bitcoin-миксерами.

На основании проведенного исследования предлагаются следующие выводы, предоставляющие практическую ценность для раскрытия и расследования преступлений, связанных с финансированием экстремистской и террористической деятельности:

Технология Blockchain предоставляет высокий уровень анонимности владельцу кошелька, однако позволяет следить за всеми транзакциями.

С помощью «пылевой атаки» появляется возможность получения оперативно-значимой информации из открытых источников.

Сотрудничество с Bitcoin-миксерами и иными организациями, предоставляющими услуги по обмену криптовалют на фиатную валюту, может способствовать раскрытию и расследованию преступлений.

Литература

1. Краткая характеристика состояния преступности в Российской Федерации за январь - март 2020 года [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/20016032/ (дата обращения: 17.04.2020).
2. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 02.12.2019) «О противодействии экстремистской деятельности» - КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=339262&fld=134&dst=1000000001,0&rnd=0.4427619338684513#09859588540401244 (дата обращения: 17.04.2020).
3. Каймак Е.В. Актуальные вопросы выявления финансирования экстремистской деятельности и терроризма // Евразийский Юридический Журнал. 2019. № 5 (132). С. 303–308.
4. Батоев В.Б., Семенчук В.В. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии Управления МВД России. 2017. № 2 (42). С. 9–15.
5. Иванов П.И. Оперативно-розыскное сопровождение противодействия финансированию экстремистской деятельности: основные проблемы и пути решения // Труды Академии Управления МВД России. 2019. № 4 (52). С. 82–89.
6. Абдулганеев Р.Р. Предупреждение финансирования деятельности религиозной экстремистской организации // Вестник Казанского юридического института МВД России. 2017. Т. 7, № 3. С.66-71. DOI: 10.24420/KUI.2017.3(29).7373.
7. Cryptocurrency Market Capitalizations // CoinMarketCap [Электронный ресурс]. URL: https://coinmarketcap.com/ (дата обращения: 17.04.2020).

К ВОПРОСУ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ МЕСТО МАССОВОГО ПРЕБЫВАНИЯ ЛЮДЕЙ

Пакляченко Марина Юрьевна[1], marina_lion@mail.ru
Гущина Анастасия Александровна[1], a.gushchina@rambler.ru

[1]Воронежский институт МВД России

Аннотация. Проведен анализ нормативной базы и предложены технические решения по обеспечению антитеррористической защищенности место массового пребывания людей с помощью технических систем безопасности.

Ключевые слова: безопасность, антитеррористическая защищенность, место массового пребывания людей, комплексная система безопасности.

На данный момент в условиях развивающейся рыночной экономики, возрастания промышленных городов, внедрения информационно-телекоммуникационных инноваций немаловажно обратить внимание вопросам организации техносферной безопасности. Указанный тип вид защищенности формируется на основе совокупного воплощения разнообразных мероприятий, превентивного характера в отношении угроз различной природы возникновения и характера проявления.

В данный момент в связи с учащенными случаями реализации террористических угроз одним из главных условий стабильной работы объектов с массовым пребыванием граждан становится обеспечение безопасности их функционирования, что приобретает все более сложный, и комплексный характер, требует определенных системных мер защиты, основанных на применении технических средств охраны (ТСО).

Во избежание реализации террористических и иных угроз необходим комплексный подход к проектированию технических систем безопасности (ТСБ), включающий в себя контроль доступа на объект, регулярный мониторинг оперативной обстановки, обеспечение пожаробезопасности и охраны жизни и здоровья людей, безопасности ценностей. Актуальной становится разработка современной технической системы обеспечения безопасности, содержащей в себе устройства и оборудование, обеспечивающее максимальную защищенность объектов, находящихся на них лиц, и реализацию указанных мероприятий.

Обращаясь к статистике, следует обозначить, что здания с массовым пребыванием людей занимают третье место после жилых зданий и складов по риску совершения террористических актов и возникновения пожара. Это обусловлено совокупностью факторов, которые необходимо рассмотреть, для того чтобы наглядно представить реальную картину антитеррористической защищенности (АТЗ), пожарной обстановки и охранного мониторинга относительно данного класса объектов.

Очевидно, что термины «место массового пребывания людей» (ММПЛ) и «место с массовым пребыванием граждан» (ММПГ) являются синонимами, разве что для последнего субъект представлен своей особой принадлежностью к государству, т. е. постоянством проживания на его территории, пользованием его защитой и обладанием в связи с этим особым правовым статусом.

Согласно законодательству под ММПЛ понимается территория общего пользования поселения или городского округа, либо специально отведенная территория за их пределами, либо место общего пользования в здании, строении, сооружении, на ином объекте, на которых при определенных условиях может одновременно находиться более пятидесяти человек.

Следовательно, к ММПГ смогут быть отнесены всевозможные здания, помещения, сооружения и территории, которым характерно одновременное пребывание свыше полусотни человек.

Составить исчерпывающий перечень подобного рода мест представляется затруднительным. Объективно к нему можно отнести административные и офисные здания, вокзалы, объекты торговли, социального обеспечения, науки и искусства, образования, здравоохранения и т.д.

Рассмотрим ряд документов, регламентирующих обеспечение безопасности и АТЗ ММПГ. Фундаментальным нормативно-правовым актом, безусловно, является Конституция Российской Федерации, в 20 статье которой определено право каждого гражданина на жизнь и охрану его здоровья (статья 7). Далее следует федеральный закон «О безопасности», определяющий

данную дефиницию, а также регламентирующий основы и принципы ее обеспечения.

Принципиально важным нормативным актом является закон «О противодействии терроризму», подчеркивающий среди принципов противодействия обеспечение и защиту основных прав и свобод, определяющий необходимость реализации технических приемов, использования техники и специальных устройств для борьбы с ним.

Регламентация указанных и иных документов, расположенных на одной ступени иерархии нормативно-правовой и нормативно-технической базы в изучаемой области носит общий характер. Конкретное определение норм, правил и требований к ММПГ содержится в Постановлении Правительства [1].

Следует учитывать, что ММПЛ включаются в перечень при соблюдении следующих условий: их правообладателями не являются федеральные органы исполнительной власти и Государственная корпорация «Росатом» или они не относятся к сфере их деятельности; они не подлежат обязательной охране Росгвардией.

Основным критерием отнесения ММПЛ к той или иной категории является количество людей, которые при определенных условиях могут одновременно находиться в ММПЛ. Их расчет, осуществляемый путем проведения мониторинга одновременного пребывания/передвижения людей на территории ММПЛ в течение 3 дней, дает представление о средней ежедневной численности посетителей ММПЛ. Плановое максимальное число определяется исходя из специфики ММПЛ, его размера и площади, занимаемой одним человеком с учетом действующих правил и стандартов, Правил противопожарного режима в Российской Федерации [2].

Постановлением определены категории ММПЛ в зависимости от возможных последствий совершения теракта и числа людей, которые могут одновременно находиться на объекте. Кроме этого в четвертой главе документа обозначены мероприятия по обеспечения АТЗ ММПЛ, среди которых отмечены применение современных технологий для обеспечения безопасности и оборудования мест необходимыми инженерно-техническими средствами.

Правилам по АТЗ ММПЛ свойственен поверхностный характер в части контроля процессов оборудования ММПЛ средствами инженерной защиты и ТСО. АТЗ мест должна отвечать типологии угроз, текущей ситуации, реализовывать максимально рациональное распределение сил и средств, обеспечивающих охрану и безопасность ММПЛ. Оборудование объекта – ММПЛ конкретными ТСО устанавливается в техническом задании на проектирование системы безопасности.

Согласно [3] КСБ – это проектируемая для конкретного объекта специализированная сложная организационно-техническая система, состоящая из алгоритмически объединенных целевых функционально самостоятельных технических подсистем и технических средств, предназначенных для комплексной защиты объекта от нормированных угроз различной природы возникновения и характера проявления. Назначением КСБ, в общем случае, является обеспечение комплексной защиты объектов от техногенных аварий, пожаров, криминальных проявлений, природно-климатических воздействий, последствий стихийных бедствий, ошибочных действий людей.

Таким образом, КСБ любого объекта, в том числе и ММПГ, с учетом его специфики может включать в себя охранную, пожарную, тревожную сигнализации, средства контроля и ограничения доступа, видеонаблюдение.

Охранные сигнализации работают вместе с иными техническими средствами защиты объекта. Так, например охранная и пожарная сигнализации, не только функционируют во взаимосвязи, но и имеют общие компоненты: каналы связи (шлейфы сигнализации), алгоритмы и протоколы приема и обработки информации, подачи тревожных сигналов и др. Благодаря этому указанные системы сигнализации объединяют в одну охранно-пожарную.

При защите крупных предприятий, банков, фирм, торговых центров и учреждений часто устанавливают параллельно сигнализации системы охранные телевизионные, которые осуществляют мониторинг и контроль объекта, а в момент тревоги верифицируют ее. Камеры и мониторы, оснащенными техническими средствами и устройствами специального назначения, могут работать в качестве извещателей (детекторов движения).

Обеспечение контроля доступа ММПГ должно реализовываться посредством системы защиты, обеспечивающей санкционированный доступ лиц на объект, разграничение полномочий прохода в помещения на определенные территории в строгом соответствии с уровнем допуска и контроль перемещения сотрудников и посетителей. Каждая из указанных систем безопасности имеет собственную специфику, которая должна найти свое отражение в общей структуре КСБ охраняемого объекта.

Проектирование КСБ по требованиям стандартов, норм и правил, необходимо реализовывать на базе технического задания, которому предшествует комиссионное обследование объекта. Обследованию подлежит вся инфраструктура объекта (рисунок 1.):

Рисунок 1. Инфраструктура объекта, подлежащая обследованию при проектировании КСБ

Разрабатываемая система должна соответствовать требованиям в части своих качественных свойств (рисунок 2.).

Рисунок 2. Качественные свойства КСБ

Таким образом, современная регламентирующая база в области безопасности позволяет реализовать проект КСБ, удовлетворяющей актуальным правилам и нормам, а передовые отечественные научно-технические разработки допускают использование на охраняемых объектах сертифицированных ТСО, отвечающих всем нормативным требованиям и обладающих высокими положительными характеристиками и параметрами.

Структура КСБ, цели и задачи отображаются на различных этапах проектирования по-разному. В этой связи крайне важно корректно сформулировать и распределить функции, организовать четкое согласование этапов разработки КСБ с учетом специфики защищаемого объекта и функционала используемых ТСО.

Целесообразно проведение работ по следующему алгоритму: характеристика объекта, его всестороннее изучение и определение индивидуальных угроз его безопасности, отработка общих вопросов о стратегии его охраны, определение реакций системы на возможные нарушения и нештатные ситуации [4]. При этом необходимо придерживаться правила о том, что спроектированная КСБ прежде всего должна удовлетворять требованиям заказчика в части реализации и экономических затрат, а также последующей эксплуатации.

Литература

1. Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий) [Электронный ресурс]: постановление Правительства РФ от 25 марта 2015 г. № 272 (с изм. и доп.) // Официальный сайт «Информационно-правовой портал ГАРАНТ.РУ». URL: https://base.garant.ru/ 70937940 / (дата обращения: 07.05.2020).

2. О противопожарном режиме [Электронный ресурс]: постановление Правительства РФ от 25 апреля 2012 г. № 390 (с изм. и доп.) // Официальный сайт «Информационно-правовой портал ГАРАНТ.РУ». URL: https://base.garant.ru/ 70170244/ (дата обращения: 07.05.2020).

3. ГОСТ Р 52551-2016. [Электронный ресурс]: Системы охраны и безопасности. Термины и определения // Официальный сайт «Электронный фонд правовой и нормативно-технической документации». URL: http://docs.cntd.ru/document/1200141714 (дата обращения: 07.05.2020).

4. Пакляченко М.Ю. Алгоритмизация процессов размещения технических средств охраны и надзора на примере объекта уголовно-исполнительной системы // Вестник Воронежского института ФСИН России. 2019. № 1. С. 107-111.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ СПОРТА

Пакляченко Марина Юрьевна[1], marina_lion@mail.ru
Масейчук Юрий Маратович[2], maratovich1990@gmail.com

[1]Воронежский институт МВД России
[2]Уфимский юридический институт МВД России

Аннотация. Обозначены актуальные вопросы обеспечения антитеррористической защищенности объектов спорта. Исследована концепция построения тактики охраны с учетом специфики защищаемого объекта.

Ключевые слова: безопасность, антитеррористическая защищенность, объекты спортивной инфраструктуры, технические система безопасности.

Объекты спорта относятся к объектам социальной инфраструктуры, они могут находиться в федеральной собственности, собственности субъектов РФ, муниципальной собственности, собственности юридических лиц, в том числе физкультурно-спортивных организаций.

В настоящее время спортивные мероприятия пользуются большой популярностью у всех слоев населения, поэтому местам их проведения характерна повышенная проходимость к обеспечению безопасного пребывания лиц, поскольку спортивные мероприятия концентрируют на трибунах значительное количество болельщиков и участников соревнований одновременно.

Особое внимание необходимо уделить антитеррористической защищенности данных объектов, так как посягательство на них вызовет как минимум серьезный общественный резонанс, а в худших исходах – массовые человеческие жертвы. В целях обеспечения безопасности персонала и посетителей объектов спорта для осуществления охраны общественного порядка согласно ряду нормативно правовых документов [1-3] объект оборудуется системой охранной и пожарной сигнализации необходимой для пресечения неправомерных действий со стороны возможных злоумышленников.

Мировая практика безопасности предполагает, что первым наиболее эффективным шагом в отношении угрозы безопасности объектов спорта яв-

ляется ее прогнозирование с целью дальнейшей нейтрализации и локализации. Для построения эффективной системы безопасности и антитеррористической защищенности спортивных объектов следует рассмотреть более подробно базовые виды угроз.

Терроризм. Это одна из главных серьезных угроз для любого масштабного события, происходящего на объекте. Пресса широко освещает спортивные события, поэтому любой террористический акт будет предан гласности и вызовет серьезную общественную и даже международную реакцию, к которой, как правило, стремятся террористы.

Преступление. Как и любое массовое мероприятие, спортивные соревнования представляют особый интерес для мелких и крупных преступных групп. Преступники пользуются преимуществами большого скопления и отдыха людей, которые увлечены спортивным зрелищем, совершают кражи из кармана, кражи личных вещей, грабежи, грабежи, мошенничество с билетами, угон транспортных средств и т. д.

Хулиганство и насилие. Хулиганы, особенно среди радикальных фанатов, являются бичом спорта уже более десяти лет. Акты насилия и хулиганства среди несовершеннолетних, к сожалению, также не редкость. Кровавые драки, угрозы, оскорбления судей и спортсменов, незаконные выходки, метание по спортивной арене бутылками, петарды, части сидений и т. д. – все это часто приводит к серьезным травмам не только среди болельщиков, но и среди спортсменов.

Чрезвычайные ситуации (пожары, обрушения, наводнения, взрывы) техногенного и иного характера. Указанные события неминуемо приводят к панике, травмам и человеческим жертвам.

К сожалению, руководители спортивных объектов не всегда уделяют должное внимание вопросам безопасности, они зачастую подходят к ним формально, привлекая к обеспечению защищенности некомпетентных сотрудников, которые не обладают навыками и теоретическими знаниями стратегии безопасности для решения этой сложной задачи. Мировой опыт показывает, что подобное попустительство может привести к значительным проблемам и невосполнимым потерям, не случайно законодательно закреплено участие государственных служб в защите объектов различной ведомственной принадлежности.

Защита небольших спортивных сооружений (спортивных залов, боулинг-клубов, бассейнов, теннисных кортов, катков) не вызывает существенных затруднений и осуществляется на тех же принципах, что и защита развлекательных центров. В случае если на спортивных объектах проводятся крупные соревнования, на которых присутствуют тысячи и десятки тысяч человек, защита строится в соответствии с дополнительными нормами и правилами.

Для обеспечения безопасности объекта необходимо выделить пять так называемых границ безопасности:

− первая граница – зона, которая окружает охраняемый объект, на расстоянии до ста метров. Контроль данной зоны обеспечивается за счет систем видеонаблюдения;

− вторая граница – периметр, где контролируется оперативная обстановка. Необходимо выявлять лиц, которые вызывают подозрения (обращать внимание на объемную ручную кладь, запрещенные к проносу предметы, ненадлежащее поведение), следует досконально изучить каждого посетителя, выявить и пресечь факты неправомерного доступа на объект;

− третья граница –специально организованная зона для осмотра вещей участников и посетители спортивных мероприятий с применением технических средств;

− четвертая граница – пункты проверки документов, а также билетов для дальнейшего следования на мероприятие;

− пятая граница – обеспечение безопасности граждан на трибунах. Безопасность обеспечивается за счет визуального осмотра граждан с целью выявления и последующего отстранения подозрительных лиц, которые могут угрожать присутствующим на объекте.

Спортивные сооружения должны быть укреплены и защищены в соответствии со строительными нормами и стандартами, оснащены современным оборудованием для обеспечения безопасности (системы видеонаблюдения, контроля доступа, пожарной сигнализации и противопожарного оборудования) и средствами инженерной защиты (ограждениями, заборами, решетками, антивандальными элементами интерьера и экстерьера).

Охрана спортивных сооружений (стадионов, ипподромов, спортивных комплексов дворцов) включает в себя следующие задачи, представленные на рисунке 1.

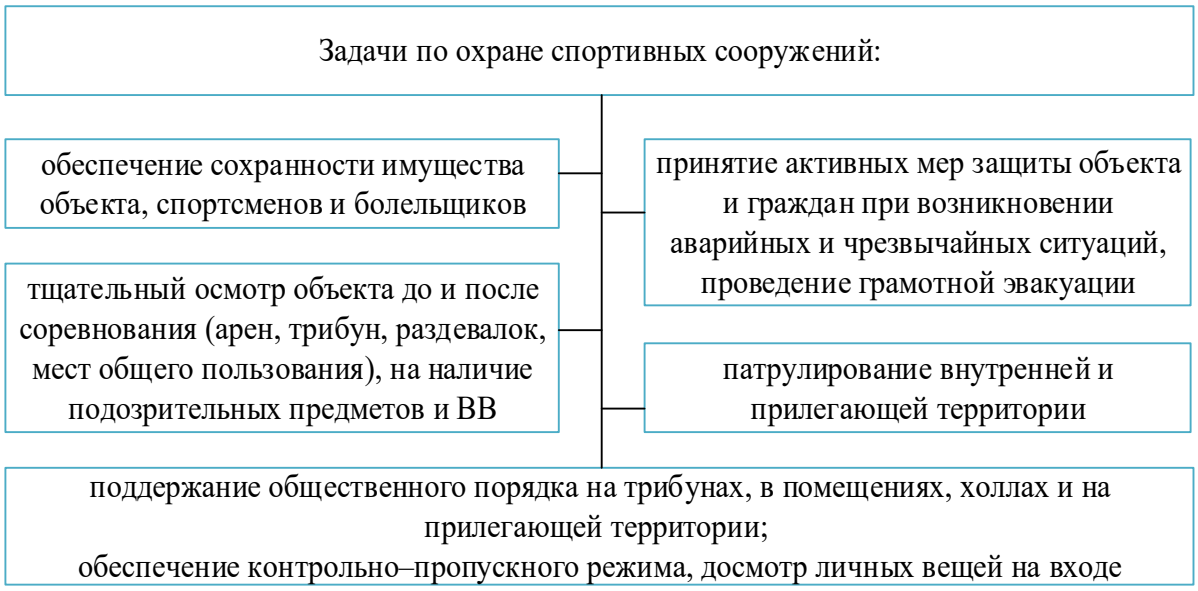


Рисунок 1. Задачи по охране объектов спорта

Для организации высокой степени безопасности необходимо провести ряд мероприятий по организации оперативной связи между всеми сотрудниками служб безопасности, компетентного управления, обеспечения коорди-

нации, распределению и перегруппировке сил в случае возникновения нештатной ситуации.

При выполнении охранных функций сотрудниками может использоваться оружие, переносные радиостанции, обеспечивающие постоянную связь, специальное оборудование для досмотра посетителей, служебные собаки для выявления проноса на объект взрывчатых, наркотических, химических веществ, а также электронное техническое оборудование (включая каркасные металлоискатели и камеры видеонаблюдения).

Объектам спорта свойственна высокая проходная способность, для выявления проноса запрещённых предметов необходимо на входе в здание устанавливать рамочные металлодетекторы. За счет выявления зоны нахождения металла у проходящих через рамку посетителя персонал охраны может быстрее определить, какой именно предмет проносит человек, что исключает возможность создания толпы на входе в здание и исключает давку.

Играет ведущую роль оперативное информирование посетителей и персонала о возможной угрозе совершения террористического акта. Своевременное реагирование на данную информацию позволит минимизировать последствия в случае совершения преступного посягательства. В случае получения достоверной информации об угрозе все лица, находящиеся на объекте, получают инструкции о правилах поведения в данной ситуации в кратчайшие сроки с использованием системы оповещения установленной в рамках оснащения здания техническими средствами охраны и безопасности.

В настоящее время безопасность объектов спорта играет важную роль в связи с возможными посягательствами не только с целью завладения материальными ценностями, но и в целях совершения теракта. Терроризм является опасным явлением, которое в современном мире находит свое проявление в различных аспектах жизнедеятельности людей. Террористические акты осуществляются с использованием не только взрывчатых веществ, но и химических составов, которые в случае их применения нанесут вред большому количеству людей. В это связи особо важным является внедрение на подобных объектах результатов достижений науки и техники, современных технологий и информационных систем.

Достижение необходимого уровня безопасности и антитеррористической защищенности объектов спорта следует реализовывать посредством применения технических средств охраны, формирующих в своей совокупности различные системы: охранно-пожарной сигнализации, контроля и управления доступом, видеонаблюдения, защиты периметра, комплексной безопасности, охранного мониторинга и др.

Литература

О порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства [Электронный ресурс]: указ Президента Российской Федерации от 14 июня 2012 г. № 851 // Официальный сайт «Информационно-правовой портал ГАРАНТ.РУ». URL: https://base.garant.ru/70189916/ (дата обращения: 07.05.2020).

Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций, а также формы паспорта безопасности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций [Электронный ресурс]: постановление Правительства Российской Федерации от 28 января 2019 г. № 52 // Официальный сайт «Информационно-правовой портал ГАРАНТ.РУ». URL: https://base.garant.ru/ 72160582/ (дата обращения: 07.05.2020).

Об утверждении требований к антитеррористической защищенности объектов спорта и формы паспорта безопасности объектов спорта [Электронный ресурс]: постановление Правительства Российской Федерации от 6 марта 2015 г. № 202 // Официальный сайт «Информационно-правовой портал ГАРАНТ.РУ». URL: https://base.garant.ru/70716970/ (дата обращения: 07.05.2020).

Гречаный С.А. Федеральные нормы и правила в области противокриминальной и антитеррористической защиты объектов: методические рекомендации. Воронеж: Воронежский институт МВД России, 2018. 65 с.

РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ФОРМИРОВАНИИ ДЕТЕРМИНАНТЫ СОЦИАЛЬНОГО ПОВЕДЕНИЯ ЛИЧНОСТИ

Шишина Елена Александровна[1], etolena8483@mail.ru

[1]Крымский филиал Краснодарского университета МВД России

Аннотация. Приведен мониторинг информационной среды на наличие информационных угроз. Проанализировано воздействие деструктивной информации на формирование установок и мировоззрение индивида, детерминанты социального поведения личности, что создает предпосылки к экстремизации населения.

Ключевые слова: информационные технологии, информационные угрозы, деструктивный контент, информационный суверенитет, формирование поведенческих шаблонов, экстремизм.

Сегодня каждый человек обладает широким спектром возможностей, связанных с доступом к новейшим технологиям и высоким уровнем глобализации информационного пространства. Наращивает свой потенциал во Всемирной сети и преступный мир, что порождает новые информационные угрозы и вызовы, в том числе и национальной безопасности.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной без-

опасности и стратегической стабильности. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

В условиях формирования «информационного общества» террористические и экстремистские организации в своей деятельности все шире используют новейшие технологии, создавая угрозу безопасности личности, общества и государства. В арсенале своих средств используют приемы психологического воздействия, как средство формирования экстремистского и террористического мышления.

Данные медиаизмерений свидетельствуют о том, что **мобильные и социальные медиа стали неотъемлемой частью повседневной жизни людей во всём мире.** На начало 2020 года в мире уже более 4,5 млрд человек пользуются интернетом - это на 7% больше, чем в прошлом году. Из них в соцсетях - 3,8 млрд. Это почти 60% населения мира. В среднем, каждый россиянин тратит 2 часа и 26 минут день на соцсети [1].

Безусловно, вовлеченность человека в Интернет-пространство, образует обширные аудитории и неограниченные возможности по скорости и возможностям распространения информации. На сегодняшний день мониторинг сети Интернет свидетельствует об использовании информационных технологий для пропаганды экстремистской идеологии. Попытки оказания спецслужбами отдельных государств информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств также представлены в информационном пространстве. Широкое распространение получило и информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей. Завоевание информационного пространства стало задачей различных групп и организаций, с целью подрыва национальной безопасности Российской Федерации.

На сегодняшний день депрессивно-(ауто)агрессивный контент составляет значительную часть содержания сотен массовых (от десятков и сотен тысяч до нескольких миллионов подписчиков) постоянно обновляемых пабликов, целевой аудиторией которых является молодежь, в первую очередь, подросткового возраста [5, с. 59]. Информационное содержание сайтов различно: тексты, графическая, звуковая информация, видеоматериалы и др.

Проводя мониторинг социальных медиа часто можно встретить суицидальный и околосуицидальный контент. Это информация, прямо призывающая к совершению самоубийств либо содержащая суицидальные риски. То есть информация, побуждающая к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью.

Просторы интернета переполнены контентом, содержащим в себе информацию, которая оказывает губительное воздействие на психику человека.

Формирует фантастическое иллюзорное восприятие мира, стремление уйти от реальности, способствует утрате мотивации к полезной деятельности, которая обычно приносит удовольствие (спорт, увлечения, культура, социальное взаимодействие и т.д.). Культивирует оторванность, отрешенность и замкнутость в реальном мире.

Широкое распространение в социальных сетях имеет так называемое «несуицидальное самоповреждение» (non-suicidal self-injury, NSSI) - селфхарм, то есть осознанные попытки навредить своему телу без намерения совершить самоубийство. Чаще всего, это самостоятельно нанесенные порезы, синяки и ожоги, расцарапывание кожи (дерматилломания), контакт с горячими предметами, прыжки с высоты и даже укусы животных, от которых человек не пытается уклониться и т.д.

Пользуется популярностью постоянно увеличивающие аудиторию приверженцы молодёжной субкультуры - сатанисты (дьяволома́ния). Сатанизм представляет собой поклонение сатане, как символу зла. Основными принципами сатанизма является потворство инстинктам, воздаяние окружающим за их заслуги вместо любви к неблагодарным, ответная месть, готовность к насилию и т.д. Сатанизм формирует богоотступничество, мизантропию. Ритуалы сатанистов связаны с вандализмом, издевательствами и жертвоприношениями животных, а иногда и людей.

Еще одна популярная молодежная субкультура - АУЕ (А. У. Е. — Арестантский уклад един (или Арестантское уркаганское единство) не сдает своих позиций в информационном пространстве. Это молодёжное сообщество пропагандирует среди несовершеннолетних воровские понятия российской криминальной среды, романтизирует преступный мир, требует соблюдения «воровского кодекса» со сбором денег на «общак», взамен обещая поддержку и защиту в настоящем и будущем. Кодекс АУЕ запрещает любое взаимодействие и помощь полиции, другим органам обеспечения безопасности и правопорядка. Сотрудники правоохранительных органов свидетельствуют о том, что на сегодняшний день уже не единичны случаи совершения имущественных преступлений молодыми людьми, причисляющими себя к сторонникам указанной субкультуры.

Широкое распространение получили колумбайн-сообщества - группы, посвященные массовому расстрелу учащихся в американской школе «Колумбайн». Эти группы распространяют информацию о радикальном движении «колумбайнеров» («скулшутинг»), призывы к массовым убийствам в учебных заведениях. До недавнего времени группы в социальных сетях, посвященные трагедии в «Колумбайне» не были запрещены. После нападений на учебные заведения в Перми, Улан-Удэ, Стерлитамаке, Керчи и т.д. многие из этих пабликов заблокировали. Но запрещенные группы продолжают жить в виртуальном пространстве под измененными названиями, администраторы некоторых пабликов заранее позаботились о резервных копиях.

В целом, деструктивный контент содержит пропаганду экстремистских взглядов, информацию, подрывающую авторитет действующей власти, призывы к массовым беспорядкам, к террористической деятельности, трансли-

рование информационных «вбросов», пропаганду безнравственного и аморального поведения, насилия, оружия и т.д. Наряду с перечисленным, культивируется феномен одиночества, безысходность, замкнутость, отрешенность, демотивация личностной активности, культ смерти, формирование взглядов «безбожия», меланхолия, ангедония, эскапизм и т.д. Анализ информационных угроз и деструктивного контента в масс-медиа и сети «Интернет», свидетельствует о том, что распространение такого рода информации, создают угрозу психическому здоровью нации и способствует радикализации населения страны.

Поведение человека реализуется через различные механизмы. Это, с одной стороны, безусловно-рефлекторные и условно-рефлекторные механизмы, определяющие непроизвольную активность человека. Человек в данном случае действует непреднамеренно, невольно, безотчетно, то есть бессознательно. С другой стороны, это произвольное управление, то есть преднамеренное, волевое, сознательное реагирование на внешние и внутренние стимулы. В этом случае может быть, как произвольная активность, вызванная потребностями и желаниями человека, так и вынужденная активность, которую человек проявляет без или против своего желания. Таким образом, потребляемый деструктивный контент, образует знание человека о мире. Соответственно совокупность знаний о мире формирует сознание.

Воздействие на психику облегчает дальнейшее внедрение желаемых поведенческих шаблонов. Состояние индивида характеризуется конформостью. То есть гибкостью мировоззренческих установок, готовностью копировать или производить изменения в поведении или мнении под влиянием реального или воображаемого «давления» со стороны отдельного участника социальной группы или всей аудитории социальных медиа. Позиция индивида становится зависимой от позиции группы. Происходит принятие или отвержение им определенного шаблона поведения, мнения, оценки, утверждения, присущих социальной группе. На смену личной идентичности приходит групповая. Как следствие, осуществление личностных перемен сообразно приемлемым установкам, мнениям, доминирующим в сообществе или группе. При этом господствующая позиция не обязательно должна быть выражена явно или даже вообще существовать в реальности. Механизм воздействия на психику индивида происходит через использование способности добиваться желаемых результатов на основе добровольного участия, предпочтений, симпатии и привлекательности для индивида. Как следствие, подконтрольность поведения индивида, позволяющая в определенный момент подтолкнуть к совершению суицидальных или наоборот, агрессивных (преступных) действий, которым, в зависимости от контекста, может придаваться - или не придаваться - общественно-политическая, религиозная или иная мотивация.

Существующий механизм запретительных правовых норм по распространению информационных угроз в настоящее время продолжает оставаться малоэффективным. Установить личность администратора групп практически не представляется возможным. Значительно затрудняет их поиск, создание

фейкового профиля, как правило, находящегося за пределами Российской Федерации. При этом на международном уровне отсутствуют правовые нормы, определяющие единые критерии оценки информационных угроз, запреты на их распространение, а также регламентированный порядок взаимодействия по противодействию информационным угрозам и киберпреступности.

Существующий механизм закрытия вредоносных групп также малоэффективен. Это довольно длительный процесс, который часто может длиться до двух месяцев. В то время, как создание резервных копий вредоносных сайтов, без труда позволяет перемещать сформированную аудиторию на другое интернет пространство, с новым названием, но с тем же содержанием, не говоря уж о скорости и масштабности появления новых деструктивных групп.

Существенно затрудняют ситуацию использование беспроводного интернета в общественных местах (транспорте, кафе, гостиницах, парках, развлекательных комплексах). Препятствует появлению информационных следов и использование так называемых анонимайзеров. Анонимайзеры (или прокси) существуют почти так же долго, как и сам интернет, и все, кто сталкивался с проблемой доступа к закрытым сайтам. Чаще всего анонимайзеры используются для доступа к заблокированным сайтам. Почти всё, что блокируется Роскомнадзором можно открыть с помощью анонимайзера. Главной функцией анонимайзера является маскировка IP- адреса, что делает присутствие в интернете анонимным. Анонимайзер работает по принципу VPN, пропуская трафик через свои серверы, которые, как правило находятся за границей. Именно физическое местоположение таких серверов позволяет анонимайзерам открывать доступ к заблокированным сайтам.

Мировой опыт свидетельствует и о том, что использование ограничения доступа к определенным интернет-ресурсам, равно как и иные методы информационной изоляции и подавления, имеют ограниченную эффективность в борьбе с использованием сети Интернет в деятельности террористических и экстремистских организаций и могут быть успешно преодолены.

Все население нашей планеты на современном этапе, являясь пользователями сети интернет вовлечено в неконтролируемый процесс порабощения, подчинения сознания манипуляционным практикам и ограничения свободы мысли. Огромные массивы информации в настоящее время не только не вызывают доверие, но и создают реальную угрозу, как отдельной личности, так национальной безопасности Российской Федерации. В связи с этим требуется выработка и реализация комплекса мер противодействия, прежде всего информационного характера, контрпропаганды.

Литература

1. Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite [Электронный ресурс]. – Режим доступа: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite/ (дата обращения 21.05.2020).

2. Иванов С.И. Проблемы профилактики радикального религиозного экстремизма и некоторые направления их решения в современных условиях / С.И. Иванов, Е.А. Ши-

шина // Актуальные проблемы теории и практики оперативно-розыскной деятельности: Материалы VII Всероссийской научно-практической конференции, посвященной 100-летию со дня образования службы уголовного розыска. - 2019. - С. 100-107.

3. Как попасть в Dark Web: пошаговое руководство и предостережения [Электронный ресурс]. – Режим доступа: https://hype.tech/@id126/kak-popast-v-dark-web-poshagovoe-rukovodstvo-i-predosterezheniya-j54nbz4j (дата обращения 21.05.2020).

4. Шишина Е.Е. «Хизб ут-тахрир аль-ислами», как фактор радикализации населения республики Крым / Е.А. Шишина// Криминалистика: теория и практика. Материалы VII Международной научно-практической конференции, 2019. - С. 365-368

5. Щербак Я. А. Предотвращение деструктивного поведения молодежи /Я.А. Щербак//Управленческие механизмы противодействия идеологии экстремизма и терроризма: материалы научно-практической конференции, 2018. – С. 58-61.