Краснодарский университет МВД России

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции

(23 апреля 2021 г.)

Краснодар
2021

УДК 316.485.6+004.7
ББК 66.4(0)+304.1
И741

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Информационные и телекоммуникационные технологии
И741 в противодействии экстремизму и терроризму [Электронный ресурс] : материалы Всерос. науч.-практ. конф. (23 апр. 2021 г.) / редкол.: А. В. Еськов, А. С. Арутюнов, К. И. Руденко и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2021. – 1 электрон. опт. диск.

ISBN 978-5-9266-1733-4

В сборнике представлены материалы Всероссийской научно-практической конференции «Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму», состоявшейся в Краснодарском университете МВД России 23 апреля 2021 г.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 316.485.6+004.7
ББК 66.4(0)+304.1

ISBN 978-5-9266-1733-4

Содержание

Аминев Фарит Гизарович,
faminev@mail.ru
Краснодарский университет МВД России

ВОПРОСЫ ДНК-РЕГИСТРАЦИИ В АСПЕКТЕ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Современный мир невозможно представить без компьютерных технологий: компьютерные технологии охватывают все сферы общества. Не является исключением и сфера судопроизводства.

По некоторым данным, активными пользователями Интернет-технологий являются более 71% населения России в возрасте старше 18 лет. Соответственно этому должен расти в обществе и уровень применения информационных технологий в правоохранительных целях, в целях раскрытия и расследования преступлений.

Так, широко известно применение в судебной экспертизе 3D-моделирования для бесконтактного сканирования и получения в трехмерном виде моделей следов и объектов, в том числе для последующего проведения с такими моделями экспертных и следственных экспериментов.

Широко применяется методика распознавания видеоизображения внешнего облика человека в режиме реального времени, разработанная на основе логического программирования интеллектуального видеонаблюдения. Это направление особенно важно для распознавания террористов, несущих непосредственную угрозу для граждан и государства. Идентификация человека по внешности производится и путем распознавания образов с применением глубоких нейронных сетей.

Имеются и другие современные высокотехнологичные информационные системы, но, в основном, иностранного производства. В этой связи полностью согласны с разработчиками методик и программ распознавания личности по видеоизображениям, которые уже не первый год предлагают создать и совершенствовать «технические средства и программное обеспечение цифровой фото-, видеофиксации внешности человека путем финансирования разработок биометрических технологий (расширив отечественные программно-аппаратные комплексы «Безопасный город» до уровня субъектов Российской Федерации и всей страны).

В этой связи хотелось бы отметить необходимость внедрения и использования отечественных информационных технологий. Решение проблем финансирования позволило бы с большей эффективностью в деле противодействия экстремизму и терроризму использовать одно из самых современных и перспективных научно-технических средств – ДНК-регистрацию.

Заниматься вопросами совершенствования системы геномной регистрации нас заставляет высказывание одного из основоположников российской криминалистики И.Н. Якимова, который криминалистическую (в начале XX века ее называли уголовной) регистрацию сравнивал с частой сетью, раскинутой над преступным миром, которая «… должна быть поставлена, по возможности, широко и всесторонне, охватывать максимальное количество учетных единиц и пользоваться точными способами учета, находящимися на высоте современной науки».

И перспективнейшим в этом направлении является реализация возможностей геномной регистрации, как системы научно–технических средств и методов по сбору, накоплению, обработке и использованию базы данных ДНК человека.

Регистрация геномов (кодов ДНК) человека имеет неоспоримые преимущества над другими видами криминалистической регистрации по ряду причин:

– для ДНК-регистрации и идентификации личности достаточно одной клетки организма (а для полноценной идентификации личности с помощью дактилоскопической регистрации необходим определенный объем дактилоскопической информации, содержащей 12 частных признаков, или, хотя бы, не менее 6; для идентификации следов обуви, орудий взлома, пуль, гильз и других объектов также необходим достаточный объем идентификационных признаков – лишь при наличии этого объема возможна идентификация);

– преимущества в устойчивости идентификационных признаков (даже папиллярные узоры, устойчивость которых гарантирована восстанавливаемостью эпидермиса, в течение жизни человека подвергаются изменениям, а геном организма неизменяем) и т. д.

Как известно, у каждого человека – свой генотип. Технические возможности оборудования, используемого в практике производства молекулярно–генетической экспертизы (фирм Promega, RapidHIT, MiSeg FGX, Applied Biosystems и др.) позволяет обеспечить результат сравнительного исследования следа биологического происхождения, изъятого с места происшествия, с образцом ДНК, полученным у конкретного человека, с идентификационной значимостью 1 из $1{,}4 \times 10^{23}$ (в то время как количество людей, когда-либо проживавших на Земле равно $1{,}1 \times 10^{11}$).

ФБР в конце 1980-х гг. разработало автоматизированную систему ДНК–регистрации CODIS (Combined DNA Index System). Но даже при отсутствии в базе данных ДНК-профиля конкретного лица удается установить с большой точностью лицо, оставившей биологический след.

Так, «в США, используя банки генетической генеалогии, правоохранительным органам удалось установить личность знаменитого Golden State Killer, который совершил двенадцать убийств и около

пятидесяти изнасилований в Калифорнии в период с 1972 по 1986 год. Первоначально секвенировали геном этого серийного убийцы из образцов ДНК, взятых с мест его преступлений. Затем отправили генетический профиль этого человека в систему генетической генеалогии – GEDmatch, где его сравнили с миллионом геномов, содержащихся в банке. Это сравнение позволило найти родственника подозреваемого. Затем генеалогическое исследование привело и к личности преступника – 72-летнего Джозефа Джеймса Деанджело, который был подтвержден тестом ДНК во время его ареста».

К сожалению, в России формирование банков генетической генеалогии не получило распространение, но зато имеется возможность с помощью ДНК-анализа установить этническую и территориальную принадлежность лица, оставившего биологический след: устанавливается, например, место рождения (Северный Кавказ или Приморский край и т. д.) и этническая группа.

Следом за США система CODIS на основе 13 STR-локусов в декабре 1998 г. была принята в Канаде, где организована соответствующая база данных ДНК Canadian National DNA Databank (NDDB), затем – в России.

Крупнейшая база данных ДНК в мире сформирована в Китайской Народной Республике – к 2019 году на геномную регистрацию были поставлены более 80 млн ДНК-профилей. Процесс создания национальной базы данных ДНК в Китае связан с принятием 3 февраля 1988 года Правил отбора проб ДНК. Важной тенденцией формирования китайской системы базы данных ДНК является ее постоянное расширение за счет включения некриминальных ДНК профилей.

Первая база данных ДНК в России была создана в 2006 году в рамках экспертно-криминалистического учета данных ДНК биологических объектов, утвержденного и регламентированного Приказом МВД от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации». Закон, регламентирующий функционирование национальной базы данных ДНК, был принят несколько позже – в 2008 году. Действующая в РФ Федеральная база данных геномной информации (далее – ФБДГИ) функционирует в соответствии с Федеральным законом от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации». Однако из-за отсутствия средств действие данного Закона было приостановлено и возобновлено только после 1 января 2011 года другим Федеральным законом №313 от 17 декабря 2009 г. Согласно ст. 2 Закона № 242-ФЗ в Российской Федерации «государственная геномная регистрация проводится в целях идентификации личности человека», каких-либо положений о раскрытии и расследовании преступлений там не указано.

Эффективность всеобщей ДНК–регистрации можно увидеть в результате следующего анализа. Так, в 2016 году 380 экспертами экспертно-криминалистических подразделений МВД Российской Федерации были проведены 62.754 молекулярно-генетические экспертизы, из которых 44.374 – способствовали установлению причастности лица к совершению преступлений. Таким образом, результативность ДНК–анализа составила 70,7%.

Специалисты ЭКП МВД РФ участвуют в осмотрах мест происшествий половины зарегистрированных преступлений (в 2016 году – 1.011.892), в 426.321 осмотров (42%) изымаются следы рук. И вот здесь особенно рельефно проявляется резерв ДНК–регистрации по установлению подозреваемых лиц: если из числа изымаемых следов рук, хотя бы по одному потожировому следу направлять на молекулярно–генетическое исследование с последующей проверкой по базе данных ДНК–регистрации, то в 70% расследуемых дел будут установлен подозреваемый (30% – потерпевшие, материально ответственные лица) – но это возможно только при условии осуществления всеобщей геномной регистрации.

При базе данных в 120.000 ДНК-профилей в 2016 году с помощью базы ДНК-учетов были установлены около 4.000 преступников. Если бы в базе ДНК содержались бы ДНК-профили хотя бы 120.000.000 человек, то и подозреваемых было бы установлено уже не 4.000, а в сотни раз больше – 400.000. Установление причастных к совершению преступлений лиц по половине нераскрытых в настоящее время преступлений было бы серьезным вкладом в реализацию принципа неотвратимости наказания и профилактику преступлений.

При осуществлении в России всеобщей ДНК-регистрации, будут решены следующие задачи:

1) установление личности людей, погибших в результате стихийных бедствий, крупных аварий, техногенных катастроф и т. д.;

2) розыск без вести пропавших;

3) опознание трупов неизвестных лиц;

4) идентификация людей, неспособных сообщить о себе какие–нибудь данные (стариков, больных, страдающих потерей памяти, малолетних детей);

5) установление лиц, причастных к экстремизму и терроризму;

6) идентификация лиц, приезжающих из стран Ближнего и Среднего Востока, Африки, Вьетнама, Кореи, имеющих одинаковые имена и фамилии, сходные внешние данные и т. д.

При наличии в базе данных ДНК-профилей всех лиц, в том числе эмигрантов, лиц без гражданства и совершающих миграционные процессы, прибывшие из зарубежья, будет реализована возможность установления всех лиц, причастных:

– к изготовлению и распространению экстремистской литературы;

– к распространению информации экстремистского содержания по сети Интернет;

– к изготовлению взрывных устройств;

– к распространению огнестрельного и иного оружия;

– к передаче денежных средств экстремистам и т. д.

В результате проведенного анкетирования студентов Института права Башкирского государственного университета «установлено, что 42,2% опрошенных считают, что изъятие биологического материала для введения в базу данных ДНК–регистрации всего населения России лучше производить при рождении; 37% – при получении паспорта; остальные называют иные возрасты (с 7 лет, с 18 лет и т. д.)».

Конечно же, для решения всесторонних, широкого спектра задач (начиная от установления факта подмены, хищения ребенка до установления личности подозреваемого) геномную регистрацию следует начинать с рождения человека путем забора биоматериала в виде мазка защечного эпителия.

Относительно разъяснения населению страны положительных моментов ДНК-регистрации всего населения при помощи отечественных разработок:

– для создания баз данных ДНК будет использоваться нейтральная информация о ДНК-снипах конкретного человека для исключения в ней любых сведений личного характера, например о болезнях и о предрасположенности к таковым.

– достигается максимальный уровень цифровизации: объем введенной в базу данных информации при ДНК-идентификации личности с помощью снипов составляет для одного человека не более 1 килобайта (с помощью STR-локусов – более 200 килобайт).

Этот метод позволяет отойти от дорогостоящих подходов, основанных на VNTR и STR-локусах, предлагаемых фирмами США и Великобританией. Осуществится уход от зависимости в иностранных технологиях и опережающее импортозамещение.

Таким образом, в результате проведения всеобщей геномной регистрации населения Российской Федерации будет создана одна из составных частей биометрической базы данных населения – база данных ДНК граждан страны, решающая задачи соблюдения интересов законопослушных граждан и государства и органично входящая в систему средств и методов противодействия экстремизму и терроризму.

Данная работа выполнена при финансовой поддержке РФФИ в рамках научного проекта-гранта РФФИ-мк № 18-29-14076 по теме «Правовые и этические аспекты всеобщей ДНК-паспортизации населения Российской Федерации для целей ДНК-идентификации личности».

Литература

1. Аминев Ф.Г. Чемерис А.В., Анисимов В.А., Сагитов А.М., Гарафутдинов Р.Р., Сахабутдинова А.Р., Хуснутдинова Э.К., Чемерис А.В. ДНК-криминалистика – зарождение, современность и перспективы // Биомика [Электронный рецензируемый журнал]. Уфа. УФИЦ РАН, 2019. том 11. № 3. С. 294.

2. Аминев Ф.Г., Анисимов А.В. Об организационном аспекте современной технологии всеобщей ДНК-регистрации граждан // Правовое государство: теория и практика. Уфа, 2020. № 2 (60). С. 16.

3. Газизов В.А., Подволоцкий В.Н. Биометрическая система как элемент развития информационного общества // Международные и национальные тенденции и перспективы развития судебной экспертизы: сборник докладов международной научной конференции, 16–17 мая 2019 г., Н. Новгород, 2019. С. 102.

4. Журавлев И.Л., Соколов А.Ю., Кадейшвили А.А. Эффективность идентификации и верификации лиц нейронной сетью при низком качестве фотоизображений. Энциклопедия Судебной Экспертизы. № 2 (13). 2017. С. 76–87. [Электронный ресурс]. Режим доступа свободный. URL: www.proexpertizu.ru (дата обращения: 20.12.2021).

5. Ищенко Е.П. Новый век криминалистики. Ч. 2. М.: Проспект, 2017. С. 280.

6. Морозов А.А., Сушкова О.С. Анализ видеоизображений в реальном времени средствами языка акторный пролог // Информационные технологии и нанотехнологии. 2016. С. 350–356.

7. Об организации использования экспертно–криминалистических учетов органов внутренних дел российской федерации [Электронный ресурс]: приказ МВД России от 10.02.2006 г. (ред. от 11.09.2018.). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 09.06.2020).

8. Чубукова С.Г. Подходы к правовому регулированию генетического тестирования в правовом государстве // Правовое государство: теория и практика. Уфа, 2020. № 2 (60). С. 152–153.

9. Якимов И.Н. Криминалистика. Руководство по уголовной технике. М.: Изд-во НКВД РСФСР, 1924. С. 31.

Арутюнов Александр Самсонович,
alexandr.arutynov@gmail.com
Краснодарский университет МВД России

Павел Андреевич Фаниев,
faniev_pavel@mail.ru
Краснодарский университет МВД России

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕКОТОРЫХ ПРОГРАММНЫХ ПРОДУКТОВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ВОССТАНОВЛЕНИЯ ЦИФРОВЫХ ДАННЫХ

Аннотация: В данной статье проводится сравнительный анализ ряда программ, предназначенных для восстановления информационных данных. Проводится их полевое испытание как в ситуации умышленного уничтожения данных (форматирования носителя информации), так и в условиях возникшего системного сбоя (нарушение целостности логики файловой системы носителя).

Ключевые слова: Recuva, R-studio, DMDE, Hetman, восстановление данных, носители информации, сбой файловой системы, форматирование.

Человек – общественное существо, обладающее разумом и сознанием, а также субъект общественно–исторический деятельности и культуры. Всю деятельность человека можно разделить на две части – материальную и духовную. Материальная деятельность направлена в первую очередь на изменение окружающей человека реальности, включая природу и общество. Духовная же имеет своей целью изменение человеческого сознания как в лице одного индивидуума, так и всего общества. Однако, в любом случае деятельность человека связана с работой в социуме. Одним из древнейших видов общественной деятельности является политическая деятельность, зародившаяся еще во времена появления первых древних греческих полисов – особая специфическая форма общественной деятельности, определяемая экономикой, но обладающая большей степенью самостоятельности, чем экономическая деятельность. К одной из особых форм ее проявления можно отнести экстремизм, смысловая нагрузка которого основана на идеологии допустимости использования крайних мер – экстремумов, для получения конкретного общественного результата. В настоящее время ученое сообщество еще не пришло к единому мнению касательно определения понятия экстремизма. Однако анализируя уже предложенные варианты, можно выделить его основные признаки:

1. насильственный захват, либо удержание власти;
2. насильственное изменение политического строя государства;

3. посягательства на общественную безопасность;

4. организация либо участие в незаконных вооруженных формированиях, сформированных для реализации вышеуказанных целей;

5. пропаганда, публичные призывы, финансирование либо иные действия, направленные на реализации пунктов 1, 2 и 3.

Опираясь на вышесказанное, можно смело утверждать, что экстремистская деятельность осуществлялась в переломные периоды истории каждого из существующих государств и реализовывалось гражданами соразмерно своим социально–техническим возможностям на том или ином отрезке времени.

Анализируя исторические факты также можно отметить, что одним из ключевых объектов, как посягательств, так и способов достижения конечной цели у экстремистов выступали средства массовой информации и средства связи. Так, например, в работе «Советы постороннего» В.И. Ленин, излагая свой примерный план организации восстания пишет: «… Комбинировать наши три главные силы: флот, рабочих и войсковые части так, чтобы непременно были взяты и ценой каких угодно потерь были удержаны: а) телефон, б) телеграф, в) железнодорожные станции, г) мосты на первую голову…».

В настоящее время одним из основных орудий экстремиста XXI века являются цифровые СМИ. Интернет – сайты органов государственной власти, видео–хостинги, социальные сети и прочие интернет ресурсы – мощнейшие инструменты воздействия на общество и, как следствие, в ряде случаев объекты хакерских атак. Однако, как и в реальной жизни, любое действие в виртуальной среде оставляет свой след, правда с учетом специфики след является цифровым.

Цифровой след (или цифровой отпечаток; англ. Digital footprint) – это уникальный набор действий в Интернете или на цифровых устройствах, которые оставляют след данных и могут идентифицировать конкретного пользователя или устройство.

Все цифровые следы делятся на активные и пассивные. К активному цифровому следу можно отнести вход на интернет ресурс через зарегистрированную учетную запись, загрузка какого-либо контента на интернет ресурс (для онлайн пространства), сохранение пароля учетной записи в памяти устройства (для офлайн пространства) или любое другое осмысленное действие пользователя.

К пассивным следам можно отнести к примеру запись в онлайн базе данных информации об IP адресе пользователя и его перемещения по сети, либо лог файлы действий, выполненных на устройстве (без персонификации лица их совершивших).

Кроме цифрового следа, колоссальный интерес представляет и сам цифровой контент, распространяемый в целях совершения экстремистской деятельности. А именно, его наличие на цифровых устройствах,

изымаемых у конкретных, подозреваемых в преступлениях лиц, поскольку данная информация может являться вещественным доказательством по уголовному делу. По этой причине преступники пытаются всячески скрыть либо уничтожить компрометирующую их цифровую информацию.

Восстановление удаленной информации – является одной из задач, решаемых при производстве компьютерной экспертизы. Для восстановления удаленных данных эксперт применяет довольно разнообразное количество специализированного софта. Исследуя алгоритмы, используемые при работе этих программ, можно заметить, что, несмотря на схожесть выполняемых задач, одни программы более успешно работают при восстановлении видеофайлов и графических данных. Другие, наоборот, более полно восстанавливают офисные документы (например, в формате .doc, .xls и .pdf). Казалось бы, ничто не ограничивает эксперта в количестве проверок диска различным программным обеспечением для наиболее полного обнаружение и восстановления всех имеющихся данных.

Возникает вопрос, зачем описывать возможности и рекомендовать тот или иной программный продукт, если эксперт при выполнении поставленной задачи может поочередно использовать каждую из программ, причем без вреда для интересующих файлов. Ответ очевиден – сроки производства экспертизы.

Руководствуясь статьей 21 Приказа МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», сотрудник может продлить сроки производства экспертизы при наличии на то объективных причин. Однако, в законе не оговариваются максимальные сроки продления. В реальности же, учитывая загруженность сотрудников государственных экспертных учреждениях системы МВД, сроки могут затянуться на 2–3 года. В силу этого складывается ситуация, когда осуществление судопроизводства в разумный срок не представляется возможным, что приводит к нарушению прав граждан, гарантированных статьей 6.1 УПК РФ.

Необходимо отметить, что от результатов экспертизы зависит не только наличие доказательственной базы, но и установление фактов, исключающих причастность лица к уголовно наказуемому деянию. По преступлениям экстремистской направленности подозреваемое лицо, зачастую, ожидает результатов экспертизы, находясь в следственном изоляторе. При этом, ввиду того что большая часть подобных преступлений является тяжким составом, срок содержания под стражей может достигать 18 месяцев. В результате мы можем столкнуться с ситуацией, когда срок содержания под стражей лица не причастного к совершению преступления, будет продлеваться по причине длительного времени производства экспертизы,

В настоящее время существует достаточно большое количество программ, предназначенных для восстановления удаленных данных, как любительских, так и профессиональных. Все они имеют различные функциональные возможное и различаются по «глубине» поиска удаленных данных. Однако, из общего массива программного продукта можно выделить своих негласных лидеров. Проведенным анализом были определены следующие программы, возможности которых будут подвергаться сравнению:

1. Hetman Partition Recovery – условно-бесплатная программа. Работает не только с исправными носителями, но и с теми, у которых имеются повреждения логических разделов. Кроме текущих разделов, программа обладает возможностью находить ранее созданные логические диски и выводить их пользователю для дальнейшего поиска и восстановления удаленных файлов. Имеет алгоритмы, способные исправлять ошибки логической структуры диска. Поддерживает чтение обычных, сжатых или зашифрованных файлов, с дисков под управлением файловых систем NTFS, FAT (32, 15, ex), ReFS. Обладает возможностью работы с RAID массивами. Поддерживает работу с USB носителями данных, а также подключаемыми по шине Sata/ATA. Из недостатков можно отметить тот факт, что программа не поддерживает специфические файловые системы, например, HFS. Кроме того, у программы отсутствует возможность сохранения результата при использовании не лицензированной версии.

2. R-studio – представляет собой набор полнофункциональных утилит для восстановления данных. Программа предназначена для работы в операционных системах Windows, Mac OS, Linux. Программа имеет широкий спектр поддерживаемых файловых систем, кроме стандартных NTFS и FAT, например UFS (ОС FreeBSD), JFS (Linux), HFS+ (Mac ОС). Немаловажным плюсом программы является возможность создания отдельной части диска в виде образа. Программа поддерживает работу с динамическими массивами RAID.

3. Recuva – утилита созданная британской компанией Pirifirm Limited. Обладает современными алгоритмами, предназначенными для восстановления не только с поврежденных или отформатированных носителей, но и несохраненных документов. Программа обладает возможностью восстановления удаленных сообщений из почтовых программ Microsoft Outlook Express, Mozilla Thunderbird и Windows Live Mail.

4. DMDE – программа для поиска, редактирования и восстановления информации на жестких дисках, RAID-массивах, flash-накопителях. Осуществляет поиск удаленных файлов, восстановление информации с поврежденных разделов, восстановление таблицы разделов. Имеет встроенный дисковый редактор, работающий с физическими носителями или их посекторными образами. Одной из особенностей

программы является возможность редактировать вручную структуру данных на диске. Имеется возможность создания посекторного копирования диска, а также обладает возможность восстановления данных с разделов, находящихся на физически поврежденных участках дискового пространства.

Программы тестировались на usb-flash носителе фирмы «Kingston». На носитель данных были загружены файлы следующих форматов: .doc, .jpeg, .pdf, .mp3, .avi. – по 10 файлов на каждый из форматов. После чего были имитированы 2 ситуации при которых возникает необходимость восстановления данных: в первом случае – сбой файловой системы, во втором случае быстрое форматирование носителя файлов. Общий объем носителя составлял 7,48 gb. Файловая система – NTFS. Программы запускались на операционной системе Windows 10 Pro.

В результате тестирования были получены следующие результаты:

Hetman Partition Recovery – в случае условного сбоя файловой системы восстановил 86% файлов (не восстановились 2 файла формата .mp3 и 5 файлов формата .avi). В случае же с быстрым форматированием восстановлены были 96% файлов (не были восстановлены 2 файла формата .avi). – время, затраченное на оба теста 1 час.

R-studio – в случае условного сбоя файловой системы восстановил 94% файлов (не восстановились 3 файла формата .avi). В случае с быстрым форматированием восстановлены были 100% файлов. Однако 2 файла формата .avi частично были повреждены и при воспроизведении часть видео ряда была утеряна. Время, затраченное на оба теста 1,5 часа.

Recuva – в случае условного сбоя файловой системы восстановить данные программой не удалось (не был определен тип файловой системы). В случае же с быстрым форматированием восстановлены были 96% файлов (не были восстановлены 2 файл формата .avi) – время, затраченное на оба теста 30 минут.

DMDE – в случае условного сбоя файловой системы восстановил 84% файлов (не восстановились 4 файла формата .jpg и 3 файла формата .pdf). В случае же с быстрым форматированием восстановлены были 100% файлов (следует отметить что в 2 файлах формата .doc при открытии был частично утерян текст, 1 изображение формата .jpg отображало только половину от изначального изображения) – время, затраченное на оба теста 50 минут

По итогам тестирования было выявлено 2 программных лидера: – R-studio и DMDE. При этом было установлено, что первая из программ по своим алгоритмам больше адаптирована для восстановления мультимедийных файлов, а другая – наоборот, больше подходит в случаях, когда необходимо сделать акцент на файлы офисных программ.

В заключение хочется отметить, что данное исследование не подводит финишную черту. Каждая из обозреваемых программ может

использоваться для выполнения задач, связанных с восстановлением массива данных. Однако полученные по итогу нашей работы качественно–временные результаты, могут помочь специалисту получить объективную оценку применяемых программных продуктов. По результатам исследований, возможно, более эффективно строить работу сотрудников экспертных подразделений и сократить время, затраченное на выполнение экспертного исследования.

Литература

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021, с изменениями от 08.04.2021) // СПС Консультант плюс URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
2. Уголовно–процессуальный кодекс Российской Федерации от 18.12.2001 № 63-ФЗ (ред. от 24.03.2021) // СПС Консультант плюс URL: http://www.consultant.ru/document/cons_doc_LAW_34481/
3. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России от 29.06.2005 № 511. СПС Консультант плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_55315/
4. Практика Европейского Суда по правам человека за 2009–2010 годы по делам в отношении Российской Федерации в связи с нарушением права на разумные сроки судебного разбирательства и/или исполнение судебного решения в разумные сроки. СПС Гарант. URL: https://www.garant.ru/products/ipo/prime/doc/12083900/
5. Типовые экспертные методики исследования вещественных доказательств. Ч. 1 / под. ред. Ю.М. Дильдина. – М.: ЭКЦ МВД России 2010. – 568 с.
6. Большой энциклопедический словарь [А.М. Прохоров]. – М.: «Большая Российская энциклопедия», 2001. – С. 544.
7. «Советы постороннего» В.И. Ленин – газета «Правда» № 250 от 7 ноября 1920 года. URL: https://www.marxists.org/russkij/lenin/works/lenin006.htm
8. Криминалистический анализ файловых систем [Брайан Керриэ]. – Спб.: Питер, 2007 – 480 с.: ил.

Арутюнов Александр Самсонович,
alexandr.arutynov@gmail.com
Краснодарский университет МВД России

Шестаков Даниил Александрович,
Daniil.tanckist@yandex.ru
Краснодарский университет МВД России

НЕКОТОРЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С ПРОВЕДЕНИЕМ СУДЕБНОЙ ЛИНГВИСТИЧЕСКОЙ ЭКСПЕРТИЗЫ ПО МАТЕРИАЛАМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Аннотация: В данной статье проводится системный анализ особенностей поводов к назначению и проведения судебной лингвистической экспертизы, рассматриваются решаемые экспертами вопросы, приводятся наиболее характерные формулировки выводов.

Ключевые слова: экстремизм, терроризм, лингвистическая экспертиза, постановление о назначении экспертизы, выводы эксперта.

Преступления, связанные с экстремизмом и терроризмом, на сегодняшний день, являются очень серьезной проблемой современного общества и его правоохранительных органов.

Согласно статистике за прошлый год, службами и подразделениями МВД России зарегистрировано 548 преступлений террористического характера, а как указывают проценты – это на 13,7% больше, чем за 2019 год. Преступлений экстремистской направленности было зарегистрировано 210, что почти на 41% больше показателей прошлого года.

Следовательно, из этого вытекает вопрос, почему так происходит?

И чтобы найти ответ на этот вопрос, необходимо понять причины подготовки и совершения преступлений, связанных с терроризмом и экстремизмом, а также выявить категории лиц, их подготавливающих.

На данный вопрос могут ответить направления некоторых экспертиз, напрямую связанных с расследованием дел по экстремизму и терроризму.

Здесь необходимо отметить такие важные экспертизы как:

- взрывотехнические экспертизы и исследования;
- баллистические экспертизы и исследования;
- судебно-медицинские экспертизы;
- лингвистические экспертизы;
- фоноскопические экспертизы;
- компьютерно-технические экспертизы;
- другие экспертизы, непосредственно используемые в расследовании преступлений в данной сфере.

В последнее время часто возникают конфликты, основанные на религиозной, национальной и этнической почве, чем активно пользуются вербовщики разных запрещенных организаций, привлекая в свои ряды как организаторов, а рядовых исполнителей актов политического противодействия.

Состав преступлений по делам об экстремизме обозначен в Федеральном законе РФ «О противодействии экстремистской деятельности» (от 25 июля 2002 года, № 114-ФЗ), а также в статьях 280 («Публичные призывы к экстремистской деятельности») и 282 («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») Уголовного кодекса РФ.

Соответственно, процесс вовлечения в свои ряды людей, связанных общим противоправным интересом, а также взглядами на мир, в преступную среду называется вербовкой.

Вербовка может происходить посредством раздач листовок, а также в сети Интернет с призывами: о публичном оправдании терроризма, с агитацией преступных действий, с пропагандой превосходства какой–то определенной нации или религии над другой, с пропагандой социальной или расовой розни, и другие вербовочные методы, носящие характер призыва к действиям экстремистской и террористической направленности.

Как правило, по данному вопросу назначают и проводят судебную лингвистическую экспертизу экстремистских материалов, объектом которой будут являться речевые произведения в форме устного высказывание либо текста, которые отобразились на любом материальном носителе, и исследуемые на предмет наличия или отсутствия в нем признаков экстремизма.

Некоторыми типичными задачами данной экспертизы являются:

– выявление и исследование информации, содержащей какие–либо отрицательные оценки или выражение неприязни к определенному полу, расе, национальности и религии;

– выявление и исследование информации, навязывающей представление о неполноценности граждан, принадлежащих к какой–либо расе, полу, национальности, а также, пропаганду призыва к действиям экстремисткой направленности;

– выявление и исследование угроз экстремисткой направленности;

– а также другие задачи, имеющие значение для решения проблем и вопросов судебной лингвистической экспертизы материалов экстремистской направленности.

Лингвистическое исследование проводится путем проведения анализа трех типов: предметно–тематического, оценочно–экспрессивного и целевого. Только при наличии трех обязательных элементов эксперт может дать категорический вывод о наличии признаков экстремизма в исследуемом объекте. К таким диагностируемым элементам относятся:

определение тематики, определение отношения и определение цели. Если отсутствует хоть одно вышеперечисленное составляющее категорического вывода, то судебная лингвистическая экспертиза может носить характер вероятностной, либо вообще не иметь доказательственного для расследования дела значения.

Первый составляющий элемент – тематика текста, ее отражает предмет речи, то есть то, в чем сам смысл текста и о чем идет речь, а также тип сообщаемой информации в нем.

Второй составляющий элемент – авторское отношение. Здесь определяется, как автор подносит идею экстремисткой направленности, как он скрывает ключевые слова и преподносит смысл текста (оправдание действия экстремисткой направленности; разделение пола, расы, национальности, религии на «свой – чужой»; подмена смысла известных высказываний в сторону экстремизма и терроризма и т. д.).

Последним ключевым элементов является цель (коммуникативная или речевая). Здесь источник призывов или пропаганды пытается сообщить адресату зачем проводится то или иное речевое действие. Таким примером может служить речевая цель инструкции, где автор пытается направить на правильное понимание его призывов к действиям, тем самым задавая определенную последовательность действий.

Аккумулируя полученные сведения и информацию о наличии признаков экстремистской направленности в тексте или в устной речи, эксперт отвечает на некоторые типичные вопросы в своем заключении:

1. Присутствуют ли в предоставленных на исследование материалах слова или высказывания с негативной оценкой социальной, конфессиональной или национальной группы?
2. Присутствуют ли в предоставленных на исследование материалах фразы, свидетельствующие о пропаганде неполноценности граждан какой–либо национальности или социальной группы в сравнении с другой?
3. Присутствуют ли в предоставленных на исследование материалах призывы к совершению насильственных или враждебных действий в отношении лиц какой–либо национальности?
4. Другие, связанные с особенностями рассматриваемого материала.

В результате исследования формируется вывод эксперта с ответами на вопросы, поставленные в постановлении о назначении судебной лингвистической экспертизы, и все материалы, связанные с расследованием преступления экстремисткой направленности, направляются для судебного рассмотрения.

Из вышеуказанного следует, что судебная лингвистическая экспертиза имеет определяющее значение при расследование преступлений, связанных с экстремизмом и терроризмом, и в дальнейшем вопросы ее производства и оценки будут находиться в центре внимания теоретиков и практиков, в контексте комплексных современных научных подходов к расследованию и изучению преступлений данных категорий.

Литература

1. Статьи 280 «Публичные призывы к экстремистской деятельности» и 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» Уголовного кодекса РФ.
2. Ф. Г. Аминев. 2017 г. По вопросу о тактике назначения судебных экспертиз при расследовании преступлений, связанных с экстремизмом и терроризмом.
3. Федеральный закон РФ «О противодействии экстремистской деятельности» от 25 июля 2002 года, № 114-ФЗ.

Гайфулин Виктор Валерьевич,
Краснодарский университет МВД России

Вайц Екатерина Викторовна,
Московский государственный технический университет
имени Н.Э. Баумана

Сычев Владимир Михайлович,
Московский государственный технический университет
имени Н.Э. Баумана

МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ КАК ИНСТРУМЕНТ ИССЛЕДОВАНИЯ КИБЕРУСТОЙЧИВОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация: Рассмотрена методика оценки угроз безопасности информации как инструмент исследования киберустойчивости объектов информационной инфраструктуры.

Ключевые слова: компьютерная атака, кибератака, киберустойчивость.

Утвержденный 5 февраля 2021 года ФСТЭК России методический документ «Методика оценки угроз безопасности информации» реализует сложившуюся на сегодняшний день концепцию определения угроз безопасности информации, возникновение которых возможно на объектах информационной инфраструктуры. Именно концептуальный характер положений данной методики составляет ее основное отличие от предыдущей версии данного документа – «Методики определения актуальных угроз безопасности информации в ключевых системах

информационной инфраструктуры» (отменена, в соответствии с информационным сообщением ФСТЭК от 15 февраля 2021 г. № 240/22/690). Он же обусловливает и целый ряд трудностей для использования методики по своему прямому назначению – для оценки уровня угрозы безопасности информации в терминах любой возможной (как правило, количественной) шкалы оценки.

Это обстоятельство существенно влияет и на возможности по оценке характеристик тех процессов, на которых, в соответствии с причинно-следственными отношениями, отражается воздействие угроз безопасности информации, а именно – на состояния защищенности информации и на эффективность информационной деятельности.

Рассмотрим основные пути преодоления этих трудностей в условиях, когда в качестве угрозы безопасности информации рассматриваются компьютерные атаки. Согласно определению [1], подобного рода угрозы возникают вследствие целенаправленного несанкционированного воздействия на информацию или получение несанкционированного доступа к ней с применением программных или программно-аппаратных средств. Как правило, в качестве таких средств используются вредоносное программное обеспечение (ВПО), разработанное на принципах компьютерной вирусологии [2]. Часто наряду с термином «компьютерная атака» применяется эквивалентный по смыслу термин – «кибератака» [3]. В этом случае процессами, на которых, в соответствии с причинно–следственными отношениями, отражаются угрозы кибератак являются процессы обеспечения кибербезопасности объектов информационной инфраструктуры, и реализуемые в ней информационные процессы. Возможности по реализации этих процессов характеризуются эффективностью защиты компьютерной информации от несанкционированного копирования, искажения информации и блокирования доступа к ней, и эффективностью реализации информационных процессов на объектах информационной инфраструктуры. Кроме того, существует еще одна весьма важная характеристика, отражающая способность объектов информационной инфраструктуры обеспечивать эффект восприятия угрозы кибератаки, как одного из допустимых состояний информационной технологии. Такой эффект достигается за счет обработки данного состояния средствами обнаружения, предупреждения и ликвидации последствий такого рода угроз. Целевой функцией этих средств является обеспечение такого уровня эффективности реализации информационных процессов, который превышал бы уровень технологического отказа [4]. Данная характеристика объектов информационной инфраструктуры определяется как их киберустойчивость [5].

Анализируя в целом «Методику оценки угроз безопасности информации» как инструмент исследования киберустойчивости объектов

информационной инфраструктуры, можно выявить два весьма серьезных обстоятельства, не позволяющих использовать ее для количественной характеристики нарушения киберустойчивости этих объектов вследствие реализации угроз кибератак на данные объекты.

Первое обстоятельство связано с доминированием эвристики вследствие экспертного подхода к оценке возможностей нарушителя по реализации угроз кибератак, основанного на анализе причинно–следственных отношений между источниками угроз, уязвимостями информации к их реализации и деструктивным воздействием. Примененный здесь эмпирический подход и описательный характер процедуры анализа способствует доминированию субъективного влияния экспертного мнения, как на сам процесс анализа, так и на достоверность его результатов, что не позволяет адекватно оценить, а, следовательно, и количественно характеризовать, нарушение киберустойчивости объектов информационной инфраструктуры вследствие реализации угроз кибератак.

Второе обстоятельство связано с тем, что «Методика оценки угроз безопасности информации» не определяет учет тех случайных состояний исследуемых процессов, которые характеризуют их динамику. Не случайно в п. 5 «Определение вероятностей реализации угроз» предыдущей версии данного документа – «Методики определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», прямо указывается на этот недостаток: «вероятность угрозы характеризует динамику ее возникновения и реализации. …Такие модели в настоящее время отсутствуют, а их разработка представляет собой достаточно длительный процесс. Для парирования сложностей, связанных с отсутствием математических моделей расчета вероятностей реализации угроз, принято следующее допущение: …вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует. Последнее допущение равносильно тому, что выбирается такое время, за которое реально существующая угроза может быть реализована с вероятностью, близкой к единице. В последующем предполагается расширить данную методику путем разработки необходимых математических моделей расчета вероятности реализации угрозы и устранить данное допущение».

Характеризуя, в этой связи, исследовательский потенциал «Методики оценки угроз безопасности информации», можно констатировать, что предпосылки для преодоления указанных трудностей заложены в п. 1.6 Методики: «На основе настоящей Методики могут разрабатываться отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности». Так, на основе приведенного в Приложении 11 Методики

перечня основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, возможно построение функциональных моделей кибератак на объекты информационной инфраструктуры. Такого рода модели позволяют детализировать последовательность действий нарушителя и последовательность реализации функций ВПО с целью достижения своих целей. Кроме того, такие модели отражают уже сложившиеся взгляды специалистов относительно сценариев реализации кибератак, основанные на выявленных закономерностях практики обнаружения, предупреждения и ликвидации такого рода угроз. Это является серьезным аргументом для отказа от процедуры экспертной оценки вариантов тактик и соответствующих им техник при построении сценариев реализации кибератак в пользу единого функционального представления такого рода угрозы, детализированного для всех возможных условий ее реализации. Примеры функциональных моделей данной предметной области приводятся в [6, 7].

Следует отметить, что функциональная модель кибератаки, кроме способа детализации выполняемых действий нарушителя и реализуемых функций ВПО, является средством формализованного представления такого рода угрозы безопасности информации. Разрабатываемые на основе данного формализованного представления математические модели временных характеристик угрозы позволяют учесть случайные состояния, представленные функциональными моделями кибератаки и процесса ее обнаружения, которые характеризуют динамику реагирования на угрозу. Примеры математических моделей временных характеристик кибератак и вероятностных характеристик реагирования на такого рода угрозы приводятся в [7–10].

Таким образом очевидно, что утвержденный 5 февраля 2021 года ФСТЭК России методический документ «Методика оценки угроз безопасности информации» содержит концепцию оценки угроз безопасности информации. Как инструмент исследования киберустойчивости объектов информационной инфраструктуры данная методика может быть использована лишь в общем виде в рамках декларируемых в ней причинно-следственными отношений между источниками угроз, уязвимостями информации к реализации этих угроз и их деструктивным воздействием, а также в рамках основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации кибератак.

Литература

1. ГОСТ Р 51275–2006: Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

2. Безопасность операционных систем: учеб. пособие для студ. учреждений высш. образования / [А.М. Сычев, Б.Н. Коробец, Е.В. Вайц и др.]; под ред. С.В. Скрыля. – М.: Издательский центр «Академия», 2021. – 256 с.

3. Киберустойчивость информационной инфраструктуры: модели исследования: монография / [В.В. Гайфулин, Е.В. Вайц, В.М. Сычев и др.]; под ред. С.В. Скрыля. – М.: КНОРУС, 2021. – 254 с.

4. Формальные аспекты представления математической модели характеристики киберустойчивости информационной среды / С.В. Скрыль, В.М. Сычев, А.В. Астрахов, В.В. Гайфулин, Ю.С. Никитина. // Промышленные АСУ и контроллеры, 2020. №3. С. 40–46.

5. Гайфулин В.В., Сычев В.М., Никитина Ю.С. Модель киберустойчивости автоматизированной системы // Охрана, безопасность, связь – 2019: сб. ст. Вып. 5. – Ч. 3. – Воронеж: Воронежский институт МВД России, 2020. – С. 130–136.

6. Скрыль С.В., Карпычев В.Ю., Потанин В.Е. Формальные основы функционального моделирования вредоносных воздействий на защищенные информационные системы в интересах выявления противоправных действий в сфере компьютерной информации // Наука производству. № 3 (89). 2006. С. 30–31.

7. Методические аспекты построения функциональной модели угроз несанкционированного доступа к компьютерной информации / С.В. Скрыль, В.В. Гайфулин, В.М. Сычев [и др.]. // Промышленные АСУ и контроллеры, 2019. № 11. С. 48–59.

8. Скрыль С.В., Сычев А.М., Мещерякова Т.В. и др. Математическая модель для оценки эффективности механизмов защиты информации от вирусных атак. Промышленные АСУ и контроллеры. – 2018. – № 4. – С. 62–69.

9. Скрыль С.В., Сычев В.М., Мещерякова Т.В. и др. Математические модели временных характеристик угроз несанкционированного доступа к компьютерной информации. Промышленные АСУ и контроллеры. – 2019. – № 11. – С. 60–65.

10. Скрыль С.В., Громов Ю.Ю., Мещерякова Т.В., Арутюнова В.И. Математическое представление показателя своевременности реагирования на угрозы безопасности компьютерной информации в условиях простейшей модели нарушителя. Инженерная физика. – 2016. – № 4. – С. 29–35.

Григорьев Анатолий Николаевич,
a.n.grigoriev@mail.ru
Калининградский филиал
Санкт–Петербургского университета МВД России

Сицская Арфения Рудольфовна,
a_sitsskaya@mail.ru
Управления МВД России по городу Волгограду

К ВОПРОСУ О ПРОФИЛАКТИКЕ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В МОЛОДЕЖНОЙ СРЕДЕ

Аннотация: В статье рассмотрены проблемы профилактики экстремизма в молодежной среде, сформулированы основные направления по профилактике молодежного экстремизма в современном российском обществе.

Ключевые слова: криминалистика, преступления экстремистской направленности, молодежная среда, профилактика, телекоммуникационные системы, сеть «Интернет».

С момента формирования основ государственности проблема экстремизма тревожит общественность, поскольку затрагивает наиболее важные сферы человеческой жизнедеятельности.

В современных российских реалиях преступления экстремистского характера представляют собой тенденцию развития общества. Анализируя статистику, можно отметить, что в 2020 году в России было зарегистрировано 2 342 преступления террористического характера, что на 29,7% больше по сравнению с 2019 годом. Число зарегистрированных преступлений экстремистской направленности выросло на 42,4% и достигло 833. Отдельно было подсчитано число зарегистрированных преступлений, совершенных с использованием информационно–телекоммуникационных технологий. По ст. 280 УК (публичные призывы к экстремистской деятельности) таких было 340 (на 32,3% больше, чем в 2019 году), 187 из них выявили в МВД, 133 – в ФСБ, два – в СК. По ст. 205.2 УК (публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма) таких преступлений было зарегистрировано 232 (+9,4%).

Проблема экстремизма является одним из факторов, угрожающих национальной безопасности и целостности страны.

Анализ ситуации, сложившейся в данной сфере, свидетельствует о том, что в настоящее время экстремистские организации и движения ведут активную вербовку новых сторонников, в том числе и несовершеннолетних, а также проводят активную работу по распространению экстремистской идеологии.

По данным МВД Российской Федерации, на учетах в органах внутренних дел Российской Федерации состоит свыше 450 молодежных группировок экстремистской направленности общей численностью около 20 тысяч человек.

В связи с этим, на фоне обострения серьезных мировых политических конфликтов, внешних угроз, изменений в социальных, духовно-нравственных, экономических и культурных реалиях, изучение проблем противодействия и профилактики преступлений экстремистской направленности именно в молодежной среде становится особенно актуальным.

Также необходимо отметить, что экстремистские организации и движения постоянно эволюционируют, корректируют или изменяют идеологию, меняют формы и методы своей работы, в том числе и по вовлечению в свои ряды новых сторонников. Зачастую с целью наиболее эффективной деятельности экстремистские организации и движения объединяются, несмотря на диаметрально-противоположную идеологию. Такими консолидирующими элементами выступают, как правило, общий враг – государство и цель – свержение конституционного строя. Это имеет свои следствием изменение как стратегии и тактики экстремистской деятельности, так и содержания распространяемой идеологии.

Для действенной и эффективной работы по профилактике экстремизма в молодежной среде, необходимо комплексное воздействие со всех сторон, оказывающих нравственное и психоэмоциональное воздействие: от учебных учреждений, до средств массовой информации и контента в социальных сетях.

Учебные учреждения, с одной стороны, являются мощным инструментом формирования сущности человека, а с другой – сигнальным аппаратом, своевременная реакция которого способна скорректировать поведение и мировоззрение подростков.

В связи с этим, одним из направлений деятельности по профилактике экстремизма в молодежной среде является проведение лекций с руководителями и воспитателями учреждений молодежной сферы, тренерами спортивных школ, центрами дополнительного образования подростков, а также других молодежных организаций.

Однако на данном этапе возникает проблема неподготовленности педагогического состава к проведению подобных мероприятий. Исключение составляют образовательные учреждения юридической направленности. Колоссальный процент преподавателей не только не обладает достаточным количеством знаний о проблеме экстремизма, особенностях его структуры, способах вербовки, но и недооценивает уровень опасности и возможных негативных последствий. Помимо этого, педагогический состав зачастую не проинформирован о возможностях противодействия проявлениям молодежного экстремизма: даже если

преподаватель замечает специфическую девиацию (опубликованные материалы экстремистской направленности в персональных аккаунтах социальных сетей или изменение в поведении, частое упоминание и приобщение себя к организациям радикальной направленности), он не знает каким образом ему стоит поступить, в какие органы обратиться, какие меры профилактики стоит применить, в связи с чем может игнорировать тревожные сигналы.

В качестве решения данной проблемы возможна разработка и реализация на уровне субъектов федерации постоянно развивающихся целевых программ дополнительного профессионального образования педагогических работников образовательных организаций как среднего общего, так и среднего специального, высшего образования по вопросам профилактики экстремизма.

Во многом облегчить и удешевить процесс может разработка универсальных методических рекомендаций для преподавателей и работников сферы образования. Особенно актуальным станет разработка информационного приложения, доступного к обращению как при помощи персональных компьютеров, так и с помощью смартфонов. Это позволит объединить достаточное количество необходимой информации, динамически изменяющейся в соответствии с трансформацией сферы запроса. В информационном справочнике подобного типа возможно будет акцентировать внимание на понимании термина экстремизм, а также возможных негативных последствиях, сформулировать методы и способы вербовки молодежи в организации экстремисткой направленности, предоставить портрет личности потенциального преступника, а также вывести алгоритм действий по профилактике и противодействию проявлениям экстремизма в молодежной среде.

Также необходимо подчеркнуть, что, помимо учебных организаций, значительное влияние на молодых людей также оказывают телекоммуникационные сети и средства массовой информации.

Тенденция преступной компьютеризации увеличивается, а условия мирового кризиса, вызванного распространением короновирусной инфекции, только способствовали данному явлению. Анализируя официальную статистику МВД Российской Федерации, необходимо отметить резкий скачек киберпреступности, а именно: за период с января по декабрь 2020 года число преступлений, совершенных с использованием информационно-телекоммуникационных технологий увеличилось на 73,4% (с использованием сети «Интернет» на 91,3%, с использованием сотовой связи – на 88,3%), а за первые два месяца 2021 года показатели возросли еще на 29,4% (с использованием сети «Интернет» на 48,3%, с использованием сотовой связи – на 32,6%).

Невозможно игнорировать тот факт, что весомый процент преступлений экстремистской направленности, а также продвижение

материалов радикального характера, вербовка в экстремистские организации происходит при помощи телекоммуникационных сетей (сети «Интернет», сотовой связи). По данным Национального антитеррористического комитета Российской Федерации, в сети «Интернет» в настоящее время работают около 200 только русскоязычных сайтов, поддерживающих идеи терроризма и экстремизма. В связи с чем, для действенных мер профилактики и предупреждения преступлений экстремистской направленности в молодежной среде необходимы качественные способы противодействия с использованием телекоммуникационных систем, в особенности сети «Интернет».

В качестве разработки мер профилактического характера с использованием средств массовой информации и телекоммуникационных сетей, можно рассматривать усиленную антипропаганду проявлениям экстремизма. Проблема обостряется тогда, когда о ней умалчивают. Свежий взгляд молодежи на тенденции развития экстремизма, существующие современные методы вербовки, а также алгоритм противодействия возможно чаще обсуждать в формате интернет–конференций. В связи с тем, что современная компьютеризации образовательного процесса привлекла на онлайн платформы приоритетную часть молодежи, организация подобных мероприятий стала значительно проще, а формат позволяет объединить представителей разных слоев населения, религий, национальностей, что позволит рассматривать проблему наиболее комплексно, однако, прежде необходимо проведение достаточной популяризации подобных мероприятий таким образом, чтобы молодые люди не только знали о факте проведения подобных событий, но и хотели принимать в них участие.

Кроме того, возможным методом профилактики преступлений экстремисткой направленности может стать анонимная онлайн площадка, куда люди могут обращаться в случаях обнаружения проявлений экстремизма в телекоммуникационных сетях или реальной жизни, получив необходимую профессиональную консультацию.

Подобная платформа способствует усилению эффективности профилактических мер, а сведения, поступившие таким образом, способны способствовать снижению пропаганды экстремизма как в телекоммуникационных сетях, так и в средствах массовой информации, и в реальной жизни.

Деятельность такого рода «платформы» способна приобщиться к работе кибердружинников. «Кибердружина» – межрегиональное молодежное общественное движение, созданное Лигой безопасного интернета в 2011 году. Оно объединяет более 20 тысяч добровольцев со всей России и стран СНГ, борющихся с преступлениями в виртуальной среде. Практическая значимость данной организации (с их помощью были раскрыты многие уголовные дела по фактам распространения детской

порнографии, сексуального насилия над детьми и иных преступлений, совершенных при помощи сети «Интернет»), а также ее распространенность (существуют официальные представительства в 36 регионах России), позволили быть сформированным законопроекту о кибердружинах, который был рассмотрен, но отправлен на доработку в 2018 году.

В настоящее время «дружинники» продолжают быть, скорее, киберволонтерами, однако, после получения официального статуса и государственной поддержки, деятельность организации способна будет привнести новые качественные изменения в части противодействия преступной деятельности в сети «Интернет», в том числе, и в качестве контрмеры распространению экстремизма.

Таким образом, на сегодняшний день проблема экстремизма в молодежной среде является чрезвычайно острой, не теряет актуальности многие годы. Для профилактики противоправных деяний подобного рода необходимо не только создание и внедрение антипропагандистского продукта, но и формирование объективного понимания проблемы у работников образовательных учреждений, поскольку они оказывают значительное воздействие на молодежную среду, а также создание консультационного продукта на привычной для молодых людей территории (в сети «Интернет») и государственная поддержка ориентированных на правовую защиту организаций.

Литература

1. Краткая характеристика состояния преступности в Российской Федерации за январь–февраль 2021 года. Сайт МВД России [электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/23447482, свободный – (01.04.2021).
2. Лига безопасного интернета. Кибердружина [электронный ресурс]. Режим доступа: http://ligainternet.ru/liga/activity-cyber.php, свободный – (16.04.2021).
3. Методические рекомендации Национального антитеррористического комитета РФ по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации / под ред. В.В. Попова. – М. 2013. – 49 с.
4. Современное состояние молодежного экстремизма в Российской Федерации. Сайт МВД России [электронный ресурс]. Режим доступа: https://есву.мвд.рф/document/3524556, свободный – (08.04.2021).
5. Состояние преступности в России за январь–декабрь 2020 года. Сайт МВД России [электронный ресурс]. Режим доступа: https://мвд.рф/reports/item/22678184, свободный – (01.04.2021).

Долгошеин Петр Сергеевич,
petrdolgoshein@mail.ru
Посольство России в Финляндской Республике

ГЛОБАЛЬНЫЕ ВОПРОСЫ, СТОЯЩИЕ ПЕРЕД ИНТЕРНЕТ-ПРОВАЙДЕРАМИ И ТРЕБУЮЩИЕ РЕШЕНИЯ ДЛЯ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ В МИРОВОМ МАСШТАБЕ

Интернет и социальные сети являются инструментом распространения экстремистских взглядов. Интернет – это доминирующее поле битвы за идеологию, борьбу с пропагандой насилия, влиянием религиозного радикализма между обществом, властями, различными силовыми структурами, организациями, вовлеченными в противодействие экстремизму с одной стороны и экстремистскими группировками с другой стороны. Группы или отдельные экстремисты с минимальными финансовыми затратами разрабатывают высококачественный контент, который с легкостью распространяются по всему миру, призывая к насилию и пропагандируя экстремистские взгляды, а также используя информационные сети для усиления террора посредством прямых стриминговых трансляций. Общество, правительства по всему миру и провайдеры технологий осознают необходимость определения и нейтрализации онлайн-контента экстремистов. Но полагаем, что проблема в осуществлении эффективного противодействия в том, что интернет-платформы открыты для всех и построены по принципу создания места для открытого диалога и обмена информацией для всех желающих без ограничений. За последние несколько лет были значительно активизированы усилия по блокированию, удалению или сдерживанию информации опасного и оскорбительного содержания, начиная от экстремизма, призывов к ненависти и безопасности детей и заканчивая обычным спамом. Инструменты для фильтрации, идентификации и реагирования улучшаются. С учетом объема контента, который сейчас передается через Интернет и социальные сети, это тяжелая работа. На парижском форуме, посвященном противодействию экстремизму в сети Интернет Мириам Эстрин из компании Google отметила, что в только в первом квартале 2018 года Google удалила 7,7 миллионов единиц контента.

Алгоритмы, разработанные специалистами компании, по-прежнему дают ошибки при категоризации опасного контента. Инженеры усиленно работают над повышением эффективности автоматических фильтров, но ошибки, связанные с выявлением опасного содержания, все еще возникают слишком часто. Удаление контента только часть решения проблемы. С технической стороны поставщики платформ вкладывают в них деньги,

интенсивно набирают и ищут методы, чтобы решить задачу. Представитель Google отметил, что вложив значительные средства в технологию машинного обучения, они автоматизировали работу, эквивалентную 180 000 человек, резко повысив скорость и эффективность проверки и удаления вредоносного контента.

Считаем, что выявление вредоносного контента до его широкого распространения – это невыполнимая на сегодняшний день задача. Различные радикальные группы маневрируют вокруг средств контроля над контентом, используя право на свободу вероисповедания и открытые площадки, на которых пользователи выражают свое мнение. Экстремисты радикализируют и вдохновляют пользователей на насильственные действия посредством своих идеологических программ, пропагандируя их легальными способами. Либеральная политика в отношении контента работает в пользу экстремистов, которые придумали, как использовать алгоритмическую модель, чтобы привлечь пользователей к своему контенту. С уровнем ресурсов, которые эти группы вкладывают в интернет–сайты и кампании в социальных сетях, это превращается в порочный круг. Даже если внедрение систем фильтрации и мониторинга вредоносного контента в виртуальном пространстве достигнет эффективного эталона надежности, то остается глобальная проблема – поддержание баланса между свободой слова и введением цензуры, направленной на строгие ограничения в Интернете и социальных сетях для охраны общественных интересов. Насколько далеко может зайти частный сектор в ограничении свободы выражения идей? Один из способов, с помощью которого можно справиться с экстремистским влиянием – разработка различных вариантов влияния на контент, помимо его полного удаления. Например, путем создания функций, которые могут исключить использование специальных возможностей видео (например, пересылки), тем самым ограничивая распространение пограничного материала.

Вопросы, которые ставят перед собой зарубежные компании:

– Должны ли они вступить в сферу редактирования и изменения контента?

– Обязаны ли они в общественных интересах бороться с радикализацией путем активного продвижения определенного нарратива?

– Где заканчивается саморегулирование компаний и берет верх социальная ответственность правительства?

В наши дни крупные технологические компании определили четкие стандарты для удаления большого количества контента, который явно или неявно является подстрекательским или опасным. Но остается открытой проблема эффективности и отсутствия двусмысленности при рассмотрении и удалении оскорбительного контента, при применении цензуры для защиты свободы выражения мнений и основополагающих принципов свободного и открытого Интернета. Учитывая срочность и

многогранность задачи, она требует участия широкого круга заинтересованных сторон и взаимодействия в мировом масштабе и, в идеале, скоординированных усилий. Полагаем, что существуют некие противоречия между саморегулированием частного бизнеса, гражданским обществом и обязанностями по контролю государственного сектора для совместной работы по противодействию пропаганде экстремизма. У государственных структур есть преимущество в использовании силовых ведомств при сборе информации, технологические компании имеют ресурсы для финансирования, гражданское общество может работать с чувствительными аудиториями, наиболее подверженными влиянию радикалов. Полагаем, что решения должны иметь комплексный и многосторонний характер.

Наблюдается рост контента, содержащего экстремизм, в Интернете, приближая глобальную интернет-аудиторию в 4 миллиарда человек к идеологии насилия, которая подрывает ценности, на которых зиждутся демократические общества – солидарность, равенство и свободу. Определены явные области, в которых онлайн-общество подпитывает рост экстремизма, способствуя распространению материалов среди пользователей интернет-сетей, подпитывая радикализацию через достижение идеологического консенсуса, укрепление движений; а также за счет учета крайних идеологических моментов, смещения целевых постов онлайн-дискуссий. Это существенно влияет на трансграничное сотрудничество между экстремистскими группами, социальные сети способствуют интернационализации маргинальных радикальных сообществ.

Способы работы экстремистских группировок в Интернете имеют много общего. Они применяют стратегию радикализации и вербовки людей, распространения пропаганды для продвижения своих идей среди новых почитателей, прежде чем продолжить процесс радикализации, привлекая новых членов в закрытые сообщества и оказывая влияние на людей посредством прямого взаимодействия. Эта динамика характерна как для исламистских, так и для крайне правых групп. Примером продвижения экстремистской идеологии является стратегия ультраправых в Германии, когда используется тактика специализированных групп по дезинформации. Показательны выборы в Германии, когда высокоорганизованные сети интернет-троллей координировали деятельность по распространению материалов, предназначенных для клеветы на их политических оппонентов, и радикализации людей в попытке поддержать партию Альтернатива для Германии на избирательных участках.

Взаимодействие в Интернете дает возможность любому принять участие в радикальной активности. Вы можете быть молодым человеком в Австралии и сделать пожертвование в пользу идеи идентичности или преследовать британского журналиста, даже не выходя из дома. Это

динамичное и энергичное влияние на пользователей, поскольку оно дает экстремистам возможность создавать общие «инструкции» для определения того, что работает и что не работает в онлайн-активизме. Поскольку в настоящее время для человека становится все более жизненно важным оказывать влияние на реальный мир посредством своей виртуальной деятельности, мы наблюдаем тенденцию, при которой интернет-культура сливается, например, с крайне правым активизмом.

Полагаем, что Интернет и социальные сети – это сфера, в которой также формируются социальные и политические субъекты. Facebook представил на своих платформах стандарты и алгоритмы сообщества, которые могут подавлять или фильтровать язык ненависти и расистские оскорбления. Одна из наиболее очевидных возможностей заключается в обеспечении механизма для создания сообществ, которые могут дать отпор поляризующим население действиям экстремистских групп. Примером этого является Инициатива гражданского мужества в Интернете, которая объединяет организации гражданского общества из Германии, Франции и Великобритании, позволяя им обмениваться знаниями и идеями. Экстремистские группы умеют создавать виртуальные контркультуры, и наша задача создавать столь же убедительные движения, которые говорят о наших общих ценностях и рассеивают ненавистническую риторику.

Скандал, возникший из-за сбора данных пользователей Facebook компанией Cambridge Analytica без согласия пользователей, заставил гигантов социальных сетей уделять больше внимания конфиденциальности и свободе слова. Какая самая большая проблема в регулировании цифрового пространства и закрытии его для экстремизма? Можно ли это сделать, не угрожая свободному и равноправному участию и одновременно вдохновляя глобальную демократическую организацию? Самая большая проблема для регулирования экстремистских материалов в Интернете заключается в принятии ответных политических мер. Полагаем, что лучший метод заключается в согласовании усилий по развитию гражданских позитивных сообществ активистов в сети, как противовес экстремисткой пропаганде.

Запрет на экстремистскую риторику на основных платформах ограничивает количество людей, которые подвергаются их вызывающей разногласия пропаганде. Однако, радикалы легко находят новые возможности для распространения своих взглядов. И такие действия стимулируют сторонников экстремистских группировок, усугубляя их недовольство. Более того, это позволяет перехватывать законные аргументы в пользу свободы слова, потенциально привлекая новых членов в свои ряды.

Полагаем, что оптимальным, является подход, который сочетает в себе реакцию правительства, гражданского общества, технологий и средств массовой информации, создавая глобальную коалицию

добровольных активистов, которые согласованно работают над деполяризацией сообществ и восстановлением дебатов у экстремистов.

Показательным примером по противодействию распространения экстремистской идеологии, применяемой в Европейском Союзе, является программа – ISDEP (Improving Security through Democratic Participation – далее ISDEP). Это новаторский проект, разработанный в партнерстве восемью странами-членами ЕС, является первым в своем роде, обеспечивающим осведомленность о противодействии радикализации практикующих специалистов по всей Европе. ISDEP разработал учебный пакет, который обучает передовых практикующих специалистов в учреждениях, занимающихся уязвимыми лицами (подверженных радикализации), распознавать, предотвращать и реагировать на все формы радикализации. Учебная программа ISDEP поддерживается всеобъемлющей программой электронного обучения на основе визуального и интерактивного изображения. Эта обучающая платформа бесплатно доступна через Интернет для практикующих специалистов на 7 европейских языках. ISDEP направлена на предотвращение обращения людей к терроризму путем устранения факторов или коренных причин, которые могут привести к радикализации и вербовке в Европе и за рубежом.

По мере изменения ландшафта глобальной угрозы, возрастает необходимость реагировать соответственно на разнообразный идеологический вызов терроризма и угрозу, с которой мы сталкиваемся со стороны тех, кто его пропагандирует. Проект ISDEP согласуется со стратегией внутренней безопасности ЕС, которая признает, что внутренняя безопасность не может быть достигнута изолированно от остального мира. Этот проект перекликается с приверженностью ЕС продвижению прав человека, демократии, мира и стабильности в государствах-членах ЕС.

Рост насильственного экстремизма во всем мире определяет необходимость укрепления институционального потенциала для реагирования на эти проблемы и повышения устойчивости персонала передового сектора. Проект сосредоточен на четырех ключевых областях противодействия экстремизму: правоохранительные органы, неправительственные организации, пенитенциарные учреждения и дополнительное образование. ISDEP повышает уровень осведомленности о процессах, ведущих к радикализации. Это позволяет распознавать, реагировать и бросать вызов идеологии и нарративам, связанным с любой формой терроризма, создавая механизм защиты уязвимых лиц.

Следующий пример – это проект **Digital Literacy –** Цифровая грамотность. Он разработан для того, чтобы научить молодых людей задавать вопросы по поводу контента, с которым они сталкиваются в Интернете, что дает возможность молодым людям распознавать некоторые приемы, которые влияют на их идеи, мнения и поведение в реальной

жизни. Сотрудники Цифровой грамотности проводят семинары с молодежью, вовлекая в процесс учителей, предоставляя им методики и обучающие тренинги, необходимые для работы в школе и создавая цифровые ресурсы, которые могут использовать преподаватели. Ресурсы на www.digitaldisruption.co.uk нацелены на поколение «коренных жителей» (11–19 лет), которые часто являются уверенными, но некомпетентными пользователями Интернета. Каждый четвертый молодой человек вообще не проверяет новый веб–сайт при посещении. Менее 1 из 10 спрашивает, кто создал сайт и почему. Треть молодых людей считает, что информация, генерируемая поисковыми системами, должна быть правдивой, а 15% основывают свое мнение о веб–сайте на том, как он выглядит и ощущается при использовании. Цифровая грамотность направлена на то, чтобы вооружить молодых людей навыками, которые им необходимы, для развития устойчивости от влияния экстремистов на просторах Интернета. Сосредоточение внимания на цифровой грамотности как средстве предотвращения радикализации в Интернете стало результатом проекта в лондонском районе Тауэр-Хамлетс в 2009 году. Проект был направлен на предотвращение радикализации молодежи в этом районе. Это произошло после того, как стало известно, что экстремистские послания были записаны на аудиокассеты и помещены в обувь молодых мусульман, когда они молились в местной мечети. Методики, используемые в Цифровой грамотности, научили молодых людей распознавать ложь и манипуляции вместо того, чтобы говорить им, во что они должны и не должны верить. Обучение сосредоточено на создании более общедоступных ресурсов в ответ на ключевые проблемы, выявленные в демонстрационном отчете 2011 года «Правда, ложь и Интернет». После того как ресурсы были подготовлены, были проведены семинары по цифровому обучению, в которых приняли участие более 500 молодых людей в Лондоне и Великобритании. Педагоги могут использовать различные ресурсы самостоятельно или в качестве расширенной программы работы по проверке источников, деконструкции пропаганды, теорий заговора и многому другому.

Как показывает международный опыт, силовые методы, направленные на выявление и удаление экстремистского контента из интернет-пространства, не являются панацеей. Необходимо применение совместных усилий государственных органов, частного бизнеса и гражданского общества. Необходимо распространять обучающие программы, которые позволяют молодежи противостоять экстремисткой пропаганде в виртуальном пространстве. Развитие технологий по введению фильтров, направленных на выявление вредоносного контента, безусловно, помогает в борьбе с экстремизмом, но, прежде всего, основным методом, обеспечивающим профилактику, является приверженность населения идеям демократического общества, плюрализм мнений и свобода слова.

Еськов Александр Васильевич,
alesc72@mail.ru
начальник кафедры
информационной безопасности
Краснодарского университета МВД России,
доктор технических наук, профессор

Селезнёв Владислав Владимирович,
студент кафедры
компьютерных технологий
и информационной безопасности
Кубанского государственного технологического университета

АНАЛИЗ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКОВ ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК

Аннотация. Описаны некоторые распространенные хакерские техники получения доступа к компьютерам жертв: использование криптолокеров и способы их внедрения, взаимодействие со средствами антивирусной защиты.

Ключевые слова: веб-приложение, атака, криптолокер, антивирусная защита, RDP-сервер.

Последними современными тенденциями является использование злоумышленниками криптолокеров, шифрующих данные на жестком диске зараженного компьютера, а также на тех сетевых дисках, на которых у пользователя есть права на запись. Как правило, за расшифровку данных злоумышленники требуют заплатить определенную сумму.

Параллельно с вредоносным программным обеспечением развиваются средства антивирусной защиты. Первые антивирусы, как и первые вирусы были достаточно примитивными. Антивирусы ранее представляли из себя определенный набор сигнатур, на основании которых программа детектировалась как вредоносная. В настоящий момент вредоносное программное обеспечение изменяется под каждую конкретную атаку с целью недопущения определения программы как вредоносной сигнатурным методом. Злоумышленники, как и обычные пользователи, имеют возможность бесплатно проверить сигнатурным методом любой файл на наличие вредоносного кода более чем 50-ю антивирусами. Одной из таких онлайн-платформ является Virustotal [1]. В связи с этим, с одной стороны время жизни вредоносного кода на настоящий момент очень короткое, а с другой стороны, злоумышленники, пересобрав вредоносное программное обеспечение, имеют возможность выявить, определяется ли вирус сигнатурным методом.

Современные средства антивирусной защиты, помимо сигнатурного анализа, используют методы эвристического и поведенческого анализа. В случае, если программное обеспечение определяется как вредоносное методами эвристического или поведенческого анализа, то данный код автоматически попадает в сигнатурную базу. В связи с этим, как правило, время «жизни» вредоносного кода составляет несколько часов.

В рамках эвристического анализа исследуется код программного продукта на предмет выявления записей, исполнение которых может привести к деструктивному воздействию (например – изменение системных файлов, внедрение в браузер и т. д.).

Если эвристический анализ можно рассматривать как некий «статический» метод, то поведенческий анализ является «динамическим» методом. Метод поведенческого анализа направлен на исследование действий программного продукта. К примеру, первоначально, на компьютер жертвы может загрузиться совершенно безобидное программное обеспечение, которое не будет определено ни сигнатурным, ни эвристическим методом. В последующим, данное программное обеспечение может загрузить другое программное обеспечение из сети Интернет, которое, в свою очередь, уже является вирусом. Соответственно, данные действия могут блокироваться методом поведенческого анализа. К примеру, для противодействия криптолокерам, средство антивирусной защиты может определять такое действие как изменение большого количества файлов в небольшой промежуток времени. В рамках поведенческого анализа определяется критичность программного продукта в зависимости от его действий в операционной системе.

В настоящее время, помимо классических антивирусов, устанавливаемых на рабочие станции, часто используются специализированные средства:

- потоковые антивирусы;
- антивирусы для прокси-сервера;
- почтовые антивирусы;
- антивирусы для облачных и виртуальных серверов;
- антивирусы для систем хранения данных (СХД) и файловых серверов.

Согласно вышеизложенной информации, существуют различные решения по противодействию вредоносному программному обеспечению. Согласно отчету Kaspersky Security Bulletin за 2020 год, [2] только антивирусные решения данной организации:

- отразили 666 809 067 атак, которые проводились с интернет-ресурсов, размещенных в различных странах мира;
- заблокировали 33 412 568 уникальных вредоносных объектов, распространяемых через web;

– отразили атаки криптолокеров у 549 301 уникальных пользователей;

– заблокировали попытки запуска вредоносного программного обеспечения, предназначенного для кражи денежных средств через онлайн–доступ к банковским счетам у 668 619 пользователей.

Указанная выше статистика получена только с антивирусного программного обеспечения Kaspersky, общее количество атак, связанных с использованием вредоносного программного обеспечения, значительно выше. Как было сказано ранее, последней тенденцией является использование криптолокеров, шифрующих информацию с целью дальнейшего вымогательства. Помимо этого, на «черных рынках» теневого интернета формируется рынок по продаже доступов в корпоративные сети. Киберпреступники, получив тем или иным образом доступ в корпоративную сеть, продают данный доступ. Покупатели используют данный доступ с целью распространения криптолокера. Данный рынок доступов в корпоративные сети только увеличивается. За период с середины 2019 года до середины 2020 года количество подобных предложений увеличилось в 2,6 раза и составило 362 лота [3]. Увеличивается и количество преступных групп, предоставляющих данные доступы – в 2020 году численность активных «продавцов» составила 63 организации (АППГ – 50 организаций). Появились также и «партнерские программы», поскольку разработчикам криптолокеров не всегда хватает компетенций для осуществления проникновения в компьютерную сеть организаций. В рамках «партнерских» отношений, разработчики криптолокеров, получив выплату от пострадавшей организации, переводят определенный процент другой киберпреступной организации, предоставившей доступ в корпоративную сеть.

С 2019 года, «фокус» киберпреступников переместился на корпоративные сети крупных организаций, а также университеты и больницы. К примеру, руководство калифорнийского университета в 2020 году объявило, что заплатило киберпреступникам 1,14 миллиона долларов за восстановление данных, зашифрованных криптолокером. Цитата из последнего абзаца публикации – «Этот инцидент отражает увеличение использования вредоносных программ киберпреступниками по всему миру в поисках денежной выгоды, включая несколько недавних атак на высшие учебные заведения». Данный инцидент произошел 1 июня 2020 года, киберпреступники использовали криптолокер NetWalker. Рекордной выплатой в 2020 году стала сумма в 4,5 миллиона долларов. Американская организация CWT, занимающаяся организацией деловых поездок и командировок, заплатила киберпрестуникам 414 биткоинов, что равнялось 4,5 миллионам долларов на момент транзакции. Известно, что злоумышленники использовали криптолокер Ragnar Locker. Следует отметить, что изначально киберпреступники требовали сумму в размере

10 миллионов долларов, однако, представителю компании CWT удалось снизить сумму выкупа до 4,5 миллиона долларов, сославшись на трудное финансовое положение из-за пандемии COVID-19. В ходе компьютерной атаки были зашифрованы данные на 30 тысячах компьютеров организации.

Согласно аналитическому отчету Hi-Tech Crime Trends 2020/2021, эксперты Group IB посчитали, что разработчики криптолокеров «заработали» не менее 1 миллиарда долларов в 2019–2020 годах. В 2020 году больше половины кибератак, связанных с использованием криптолокеров, осуществлялось через удаленное внешнее подключение. На долю фишинговой атаки отводится 29% всех атак (рис. 1).

Рис. 1. Первичный вектор компрометации

Рассмотрим, каким образом злоумышленники осуществляют удаленное внешнее подключение. Пандемия COVID-19 вызвала необходимость у большинства предприятий организовать для своих сотрудников режим удаленной работы. В связи с этим, удаленное внешнее подключение киберпреступниками осуществлялось через публично доступные RDP-серверы. Основной вектор атаки происходил по следующей схеме – в ходе сканирования сети Интернет, злоумышленники выявляли общедоступный опубликованный RDP-сервер. Определив организацию-владельца сервера, киберпреступники осуществляли сбор учетных записей сотрудников организации (например – IvanovII@<domain name>.com.). После сбора информации осуществлялась попытка подбора паролей или подстановка скомпрометированных вверительных данных. После установления соединения, атакующие продвигались по сети предприятия к контроллеру домена. Подобные векторы атаки также применялись также и в отношении к VPN, если в организации не была внедрена многофакторная аутентификация.

Помимо взлома RDP-серверов или VPN, согласно рис. 1, злоумышленники в 29% случаев использовали фишинговые письма. Данная атака была опробована еще в 2017 году, когда для первичной компрометации использовался троян Dridex с целью дальнейшего

функционирования криптолокера BitPaymer. Фишинговые письма используются непосредственно для доставки трояна на целевые хосты атакуемой организации. В письме могут быть расположены как фишинговые ссылки, так и вредоносные вложения в различных форматах, начиная от офисных документов и заканчивая исполняемыми файлами, архивами, скриптами.

Опытный специалист по информационной безопасности сразу определит, что письмо является фишинговым. Об этом может свидетельствовать некорректный адрес электронной почты отправителя, наличие ссылок в теле письма на неизвестные ресурсы, угрожающий текст в сообщении или информирование пользователя о том, что нужно в кратчайшее время сделать то или иное действие. Неинформированный пользователь может быть невнимательным или испугаться и в итоге открыть вложение, полученное от неизвестного источника или перейти по ссылке.

Тем не менее, не все киберпреступники использовали фишинговые атаки. Известная атака Badusb, совершенная группой Fin7, заключалась в том, что злоумышленники присылали письма по обычной, бумажной почте от имени компании BestBuy. В письме находился поддельный подарочный сертификат на 50 долларов и зараженный USB флэш-накопитель. В письме сообщалось, что на флешке находится список товаров, которые можно оплатить с помощью сертификата.

Для закрепления на скомпрометированных хостах часто используется планировщик задач Windows. К примеру, участники партнерской программы Maze для запуска криптолокера в определенное время создавали запланированные задачи, замаскированные под обновления системы безопасности.

Для сохранения доступа к скомпрометированным системам использовались также следующие техники:

– вредоносное программное обеспечение добавлялось в автозагрузку и в раздел реестра Run;

– создавались дополнительные учетные записи (команда net user);

– создавались новые службы Windows;

– использовались не отключенные учетные записи (например Гость или локальный администратор).

Для повышения привилегий злоумышленниками используются следующие техники:

– обход контроля учетных записей (UAC-Control). Например, чтобы обойти UAC в системе с Windows 10, Trickbot модифицировал разделы реестра сначала с помощью fodhelper.exe, а затем – wsreset.exe;

– использование уязвимостей программного обеспечения. Например, в некоторых случаях для повышения привилегий до системных на скомпрометированном хосте разработчики криптолокера ProLock

применяли эксплойт для уязвимости Windows CVE-2019-0859. Другим «примером» могут служить разработчики шифровальщика REvil, которые для повышения привилегий эксплуатировали уязвимость CVE-2018-8453;

– внедрение программного кода в процессы. Для операторов SDBbot, например, характерно внедрение динамической dll-библиотеки в процесс rundll32.exe. Та же техника используется во многих других программах–вымогателях. Например, шифровальщик Netwalker внедряет DLL в процесс explorer.exe;

– дампинг учетных записей. С помощью инструмента Mimikatz злоумышленники применяли различные варианты техник дампинга учетных данных, включая дампинг памяти LSASS или диспетчера учетных записей безопасности SAM, хранилища LSA Secrets или кэшированных учетных данных.

Хакерских техник, в том числе и весьма оригинальных, достаточно много. К примеру, некоторые преступные группы на компьютере жертвы создавали виртуальную машину Windows XP/7, на которой монтировали сетевые диски и запускали криптолокер минуя все средства защиты (например – антивирусы), используемые на «родительских» операционных системах.

Литература

1. Бесплатный онлайн сканер вирусов [Электронный ресурс] – URL: https://www.virustotal.com/gui/home/search

2. Kaspersky Security Bulletin 2020 [Электронный ресурс] – URL: https://securelist.ru/ksb–2020/

3. HI–TECH CRIME TRENDS 2020/2021 [Электронный ресурс] – URL: https://blog.group–ib.ru/trends20_21

Еськов Александр Васильевич,
alesc72@mail.ru
Краснодарский университет МВД России

Селезнёв Владислав Владимирович,
Кубанский государственный технологический университет

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ МЕТОДОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ–ПРИЛОЖЕНИЙ OWASP

Аннотация. Описана методология анализа и описания критичных рисков безопасности веб-приложений OWASP. Проведен обзор способов противодействия экстремизму в сети Интернет с использованием описанной методологии.

Ключевые слова: веб-приложение, информационные риски, методология, OWASP, PTES.

На этапе разработки веб-приложений продумываются способы обеспечения безопасности данных в приложении. Использование сложных паролей и защищенных соединений бывает недостаточно, поскольку существуют множество векторов атак, использующих всевозможные программные уязвимости. Используя наиболее опасные и распространенные уязвимости могут использовать операторы служб поиска и анализа информации экстремистского содержания в сети Интернет (рис. 1).

Любое веб-приложение представляет собой набор статических и/или динамических веб-страниц. Статическая веб-страница – это страница, которая всегда отображается перед пользователем в неизменном виде. Веб-сервер отправляет страницу по запросу веб-браузера без каких-либо изменений. В противоположность этому, сервер самостоятельно генерирует динамическую веб-страницу (на основании серверных скриптов) перед отправкой ее браузеру.

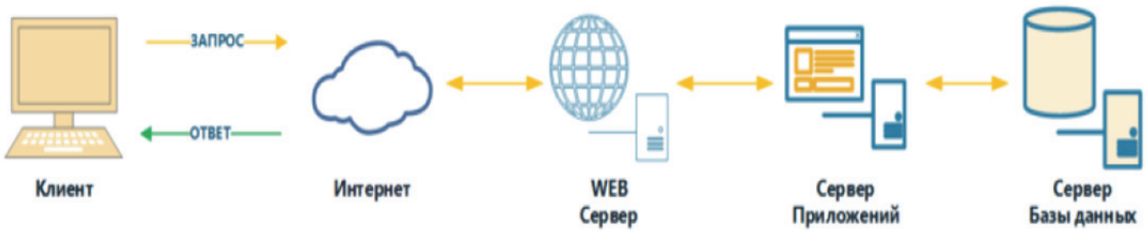


Рис. 1. Схема работы веб–приложения

OWASP (Open Web Application Security Project) – это открытый проект обеспечения безопасности веб–приложений, который занимается анализом и методами улучшения информационной безопасности веб-приложений. Топ-10 уязвимостей, представленных в OWASP, представляет полный перечень наиболее критичных рисков безопасности веб-приложений и отражает проблемы в области информационной безопасности [1, 2].

Используя терминологию информационной безопасности веб–приложений – уязвимости веб-приложений могут эксплуатироваться операторами в ходе проведения компьютерной атаки. Компьютерные атаки могут значительно отличаться друг от друга применяемыми техниками, но, тем не менее, осуществляются по схожим методологиям.

Процесс определения уязвимостей обозначен в различных методологиях, таких как PTES, OWASP и т. д. Указанные методологии могут использоваться как специалистами по тестированию на проникновение, так и операторами. Исследуем методологию OWASP с точки зрения составления модели действий оператора.

Последней действующей версией методики является OWASP Testing Guide v4. Данная методика разработана под тестирование именно web-приложений и является наиболее актуальной на сегодняшний день.

Методика OWASP содержит в себе следующие разделы:

- введение;
- руководство по тестированию OWASP;
- тестирование на проникновение web–приложений;
- составление отчета.

Методика OWASP разработана для пентестеров, но может использоваться и операторами. По мнению создателей, с данной методикой должны быть ознакомлены разработчики для создания безопасных приложений, тестировщики программного обеспечения для расширения набора текстовых примеров, которые они применяют, специалисты по безопасности для анализа уровня защищенности web–приложения и руководители проектов с целью понимания причин формирования проблем с безопасностью.

Согласно методике OWASP, процесс атаки можно разделить на два этапа – пассивный и активный. Во время пассивного этапа оператор ставит своей целью определить логику работы web–приложения. На данном этапе могут использоваться различные инструменты, такие как перехватывающие прокси (Burp Suite и OWASP ZAP). С помощью данных утилит оператор видит все запросы к веб–серверу и полученные ответы. Целью пассивного этапа является определение всех точек входа в приложение (передаваемые параметры, http-заголовки, cookie). К примеру, оператор может получить url страницы аутентификации – https://test.site/index.php?login=admin&password=Pa$$w0rd. В таком случае

параметры login и password являются «точками входа» в приложение. Оператор может отправлять какие угодно значения в указанных параметрах и анализировать ответ web-сервера.

В методике OWASP рекомендуется составить таблицу со всеми установленными точками входа для дальнейшего тестирования. В таблицу также необходимо добавлять методы отправки (как правило GET и POST). Если используются методы PUT или DELETE, то на них нужно обратить особое внимание.

Согласно методологии OWASP, существуют прямые и непрямые методы получения информации. Прямые методы означают получение сведений непосредственно на исследуемом web-приложении. В то время как непрямые методы означают, что сбор информации происходит на других ресурсах (google, shodan и т. д.). В случае ошибок конфигурирования или отсутствия актуальных обновлений для файла robots.txt, поисковым роботом могут быть проиндексированы страницы, которые не предназначены для общего доступа. К рекомендуемым инструментам на этапе сбора информации относятся FoundStone SiteDigger, Google Hacker, Bishop Fox’s Google Hacking Diggity Project, PunkSpider.

В рамках сбора информации важным этапом является определение версии web-сервера. Зная версию и тип используемого web–сервера, атакующий может определить актуальные уязвимости.

В ходе сбора информации необходимо проверить исходный код на наличие комментариев. Подобный функционал позволяет осуществить программное обеспечение OWASP ZAP.

Определение структуры web-приложения, используемого framework (или CMS) также относится к этапу сбора информации. По итогам сбора информации создается карта архитектуры web-приложения. Вышеуказанные сведения необходимы атакующему для дальнейшей атаки.

Корректное конфигурирование инфраструктуры является важной частью общей безопасности web-приложения. Если какой-либо компонент web–приложения содержит в себе ошибки конфигурирования, то это может использоваться оператором. Для определения ошибок оператор может осуществить следующие действия:

– определить компоненты инфраструктуры web-приложения, а также определить, как они влияют на безопасность приложения;

– проверить все компоненты инфраструктуры на наличие известных уязвимостей;

– определить список сетевых портов, необходимых для функционирования веб-приложения, а также отслеживать возможные изменения в этом списке.

После процедуры сбора информации оператор проверяет web-приложение по нижеуказанному плану:

- сбор информации;
- тестирование конфигурации;
- тестирование пользовательской безопасности;
- тестирование аутентификации;
- тестирование авторизации;
- тестирование управления сессией;
- тестирование обработки пользовательского ввода;
- обработка ошибок;
- криптография;
- тестирование бизнес-логики;
- определение уязвимостей на стороне пользователя.

Представленная методология анализа и описания критичных рисков безопасности веб-приложений OWASP позволит оператору обнаружить уязвимость и в дальнейшем проанализировать информацию, предназначенную для генерации динамических веб-страниц.

Литература

1. Виртуальная система OWASP [Электронный ресурс] – URL: https://owasp.org/www-project-broken-web-applications (дата обращения: 03.05.2021).

2. Список OWASP Top Ten [Электронный ресурс]. – URL: https://owasp.org/www-project-top-ten (дата обращения: 05.05.2021).

Жилин Роман Андреевич,
zhilin99.zhilin@yandex.ru
Воронежский институт МВД России

О РАЗЛИЧНЫХ ПОДХОДАХ ПРИ РАЗРАБОТКЕ МОДЕЛИ НАРУШИТЕЛЯ СИСТЕМ БЕЗОПАСНОСТИ

Статья посвящена обзору различных подходов при разработке модели нарушителя систем безопасности.

Разработка модели нарушителя нашла применение в области информационной безопасности, а также в сфере охраны объектов уголовно-исполнительной системы и транспортной инфраструктуры.

Модель нарушителя на законодательном уровне рассматривается лишь в методических документах ФСБ и ФСТЭК.

В научно-технической литературе модель нарушителя представлена несколькими способами:

1) в виде классификации признаков;

2) описательным методом;

3) математической моделью;

4) с помощью программирования;

5) комбинацией данных способов;

6) при помощи логически выстроенной иерархической структуры (алгоритма).

В виде классификации признаков модель нарушителя представлена в работах А.В. Ничикова [1], А.П. Стефарова [2] и Р.Г. Магауенова [3].

А.В. Ничиков в работе использует понятие модели нарушителя и ее применение в задачах обеспечения транспортной безопасности. Вводит понятие проектной модели нарушителя, раскрывает типажи нарушителей. Проектная модель нарушителя описывается в текстовом виде, либо в виде таблицы с подробными характеристиками, также описывается ее применимость на различных объектах транспортной инфраструктуры.

Модель нарушителя по А.В. Ничикову может быть сформулирована, как перечень проектных характеристик для каждого типа нарушителей с реализуемыми ими угрозами. Для создания модели действий нарушителя в данной статье рассматриваются категории нарушителя.

В публикации А.П. Стефаров при помощи нормативно-правовых актов ФСБ и ФСТЭК рассматривает несколько классификационных признаков нарушителя информационной безопасности. В результате формируется 6 категорий внутренних потенциальных нарушителей с подробным описанием их параметров.

Далее А.П. Стефаров делает вывод, что уровень знаний внутреннего нарушителя зависит непосредственно от функциональных обязанностей нарушителя. В качестве критерия классификации, позволяющего классифицировать нарушителей, предлагается использовать уровни воздействия нарушителя.

А.П. Стефаровым в публикации создана таблица соотношения категории нарушителя и уровней воздействия нарушителя, в результате которой, данные из таблицы позволяют классифицировать предполагаемого нарушителя информационной безопасности.

В статье также описаны критерии при формировании типовой модели нарушителя, которая представлена шестью категориями.

Р.Г. Магауенов в пособии под моделью нарушителя понимает совокупность полученных оценок (пути возможного проникновения нарушителя, интерес, технические возможности и т. д.).

В учебном пособии представлена классификация нарушителей по уровню их технической оснащенности, раскрывается понятие неподготовленного нарушителя, описываются варианты проникновения нарушителя на охраняемый объект. Также рассмотрена классификация нарушителя на основе модели действий.

С течением времени и развитием современных технологий, модель нарушителя, как и вся концепция охраны, могут изменяться.

По мнению Р.Г. Магауенова для разработки модели нарушителя, необходима совокупность опыта отечественной и зарубежной практики проектирования систем безопасности объектов.

Разработка модели с позиции Р.Г. Магауенова должна реализовываться на основе исследования потенциальных угроз объекту и способов их осуществления.

Р.Г. Магауенов подробно описывает нарушителей 3 типов, рассматривает 2 группы способов реализации угроз, классифицирует способы проникновения на охраняемый объект и условия, которые могут этому проникновению способствовать.

Информация о способах проникновения потенциального нарушителя на охраняемый объект должна иметь определенный гриф секретности.

В пособии приводится классификация контактных и бесконтактных способов совершения враждебных действий в отношении охраняемого объекта.

Для описания модели нарушителя в качестве критериев классификации Р.Г. Магауенов рассматривает потенциальные цели и задачи нарушителя. На основе критериев делит нарушителей на 4 категории.

Также существуют статьи, где модель нарушителя представлена описательным методом, который рассмотрен в публикациях Н.В. Гришиной [4], А.В. Богданова [5], И.Р. Зулькарнеева [6].

В статье дается определение нарушителя безопасности, а также приводится классификация на внешнего и внутреннего.

А.В. Богданов выделяет 6 типов нарушителей с подробными описательными характеристиками. Определение конкретных значений данных характеристик модели в значительной степени являются субъективными.

И.Р. Зулькарнеев считает, что результатом создания модели нарушителя является описание возможностей нарушителя безопасности.

Идеей публикации является объединение моделей нарушителя по методикам ФСБ и ФСТЭК. При создании объединенной модели, по мнению И.Р. Зулькарнеева, необходимо из всех обобщенных возможностей выбрать наиболее актуальные.

Математической моделью нарушитель представлен в статьях Г.Н. Гудова [7], С.В. Скрыля [8], В.А. Гриненко [9] и О.Т. Даниловой [10].

Г.Н. Гудов рассматривает математическую модель действий нарушителя информационной безопасности.

В.А. Гриненко в публикации подробно рассмотрел параметры предполагаемого нарушителя при разработке математической модели. В работе предъявлены требования к разработке модели, упоминается понятие нарушителя, а также перечислены факторы, влияющие на значение параметров модели нарушителя.

Модель нарушителя с математической точки зрения может принимать качественный или количественный параметр. Но на практике, как правило, используют комбинированную модель, в которой сочетаются элементы тех и других параметров.

В статье представлена формула скорости рассматриваемого в модели нарушителя:

$$V = k_n v_0$$

где:

k_n – коэффициент профессионализма нарушителя;

v_0 – скорость бега нарушителя (4 м/с)/

Также в статье представлен сценарий поведения нарушителя в виде графа.

Для апробации полученного алгоритма О.Т. Данилова рассматривает гипотетическую систему физической защиты, внешнего нарушителя, который обладает низким, средним или высоким потенциалом.

При помощи комбинаций различных способов модель нарушителя в статьях рассматривают В.И. Белоножкин [11] и Я.Н. Немов [12].

По мнению Я.Н. Немова при построении модели потенциального нарушителя и сценариев возможного поведения целесообразно учесть совокупность различных факторов и критериев. Совокупность угроз представлена в виде математического множества, которое содержит в себе проектируемые угрозы.

Я.Н. Немов считает, что стратегия действий нарушителя зависит от различного рода факторов и их параметров. В статье подробно описываются характеристики потенциального нарушителя объекта ФСИН и приводится классификация стратегий его действий.

Встречаются научные статьи, где модель нарушителя представлена с помощью логически выстроенной иерархической структуры, которая является одним из элементов при разработке модели нарушителя.

Например, В.И. Белоножкин использует иерархическую структуру для систематизации данных о типологиях, возможностях и целях нарушителя безопасности.

Н.В. Корнеев [13] использует структурную схему при моделировании маршрута нарушителя к цели «Генеральный директор», для дальнейшего построения графа на основе модели угроз и категорирования предполагаемого нарушителя.

В основном данный подход используется при комбинированном способе моделирования, в целях наглядного представления описанных характеристик, параметров.

Литература

1. Белоножкин В.И. Модель нарушителя безопасности региональной антитеррористической ИАС / В.И Белоножкин // Информация и безопасность. Т. 9. № 2. – 2006. – С. 155–157.
2. Богданов А.В. Неформальная модель нарушителя безопасности объектов культуры / А.В. Богданов, И.Г. Малыгин, Ю.И. Синещук // Научно-аналитический журнал вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России. № 3. – 2013. – С. 109–113.
3. Гриненко В.А. Общий подход к описанию параметров модели нарушителя // Спецтехника и связь. № 1. – 2011. – С. 22–25.
4. Гришина Н.В. Модель потенциального нарушителя объекта информатизации // Известия ТРТУ. № 4 (33). – 2003. – С. 356–358.
5. Гудов Г.Н. Математическая модель действий «нарушителя» информационной безопасности / Г.Н. Гудов, О.С. Купач // Технологии техносферной безопасности. № 4 (56). – 2014. – С. 24–31.
6. Данилова О.Т. Алгоритм построения модели нарушителя на примере системы физической защиты с применением теории игр и теории графов / О.Т. Данилова, С.О. Савченко, Н.В. Капчук // Омский научный вестник. № 4 (154). – 2017. – С. 115–119.
7. Зулькарнеев И.Р. Объединение методик создания модели нарушителя по требованиям ФСТЭК и ФСБ / И.Р. Зулькарнеев, Ю.А. Кибардина, М.С. Тякунов // В сборнике: безопасность информационного пространства Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Министерство образования и науки Российской Федерации Координационный совет по подготовке (переподготовке) и повышению квалификации кадров в области защиты информации в Уральском федеральном округе федеральное государственное бюджетное образовательное учреждение высшего образования «Курганский государственный университет». – 2016. С. 78–81.
8. Корнеев Н.В. Программное средство для оценки антитеррористической и противокриминальной защиты объектов / Н.В. Корнеев, Ю.В.Колесникова // Известия Самарского научного центра Российской академии наук, т. 16, №4, 2014. – С. 109–115.
9. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: учеб. пособие / Р.Г. Магауенов. – М.: Горячая линия – Телеком, 2004. – 367 с.
10. Немов Я.Н. Модель нарушителя и стратегий его действий в системе физической защиты объекта ФСИН России // Вестник Воронежского института МВД России. № 2. – 2012. С. 187–195.

11. Ничиков А.В. Понятие «модель нарушителя» и его связь с задачами обеспечения транспортной безопасности // Мир и безопасность № 3, 2014. – С. 14–18.

12. Скрыль С.В., Исаев О.В. Имитационное моделирование процесса преодоления «моделью» нарушителя комплексов средств охраны // Вестник Воронежского института ФСИН России, 2013, № 1. – С. 65–67.

13. Стефаров А.П., Жуков В.Г. Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах // Известия ЮФУ. Технические науки. № 12 (137). – 2012. – С. 45–54.

Ивличев Павел Сергеевич,
psi940@mail.ru
Рязанский филиал
Московского университета МВД России
имени В.Я. Кикотя

ВОЗМОЖНОСТИ ТЕХНИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ИНФОРМАЦИИ, ОБОРОТ КОТОРОЙ ЗАПРЕЩЕН В РОССИЙСКОЙ ФЕДЕРАЦИИ

Российское информационное право базируется на принципе свободы оборота информации, который установлен статьей 29 Конституции Российской Федерации. Однако, очевидно, что такой режим все равно нуждается в регулировании, поскольку существует информация ограниченного доступа, а также существуют категории информации, распространение которых крайне нежелательно.

Эта нежелательность может быть обусловлена стремлением сохранить информационное спокойствие граждан, а также противодействовать ряду преступлений в информационной сферы.

Федеральное законодательство относит к категории запрещенной к распространению информации следующие виды:

– информация, направленная на пропаганду войны;

– информация, направленная на разжигание национальной, расовой или религиозной ненависти и вражды;

– иная информация, за распространение которой предусмотрена уголовная или административная ответственность.

Если последняя категория, в силу того, что за ее распространение предусмотрена конкретная ответственность, дает возможность правоохранительным органам предпринимать достаточно широкий спектр действий, то относительно информации первых двух видов закон оставляет только возможности мягкого противодействия путем

ограничения доступа к информационным ресурсам, распространяющим такую информацию.

Следует отметить, что такое мягкое противодействие по умолчанию не может являться эффективным. Это связано с тем, что принимая к использованию какую-либо технологию, государство принимает все достоинства, недостатки и особенности данной технологии. Несмотря на серьезные попытки правового регулирования сети Интернет, которые принимаются в Российской Федерации с 2012 года, эффект от этого регулирования остается сравнительно невысоким.

Теоретически, функционирование Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, выглядит логически выверенным и продуманным. Оператор реестра, выявив запрещенную к распространению информацию, уведомляет об этом провайдера хостинга, который сообщает о претензиях владельцу сайта. Далее владелец сайта для того, чтобы избежать внесения сайта в реестр, должен удалить запрещенную информацию.

Если же владелец сайта это не сделал, то заблокировать доступ к сайту должен провайдер хостинга. Это действенная мера, поскольку приостановка оказания услуг хостинга гарантированно прекращает доступ к сайту. Однако, эта схема не работает в том случае, когда владелец хостинга изначально не собирается соблюдать российское законодательство или сознательно допускает нарушения, предоставляя, к примеру, свои ресурсы для ведения экстремистской деятельности. Правового способа воздействовать на такого провайдера хостинга не существует, а организационная мера в виде включения сайта в реестр оказывается неэффективной из-за особенностей функционирования сети Интернет и возможности выполнения косвенных запросов.

В качестве инструментов для косвенных запросов используются прокси-серверы, виртуальные частные сети и анонимные сети.

Западные страны при борьбе с распространением нежелательной информации эффективно используют экономические методы, блокируя счета владельцев сайтов и провайдеров хостинга, на которые перечисляются доходы от реферальных программ. Однако, для эффективности этого метода в России необходим развитый и значимый национальный сегмент сети Интернет, а также развитый сетевой банковский сектор, что не соответствует действительному положению вещей.

Затруднительность решения проблемы юридическими и экономическими методами заставляет искать иные пути решения проблем. Жесткий контроль за распространяемой в сети Интернет информации, вплоть до полного запрета трансграничного трафика в настоящее время на

территории России невозможен, что опять же связано с технологическими особенностями реализации доступа к сети Интернет в нашей стране. Развитие национального сегмента сети происходило в 90-е годы, без существенного государственного участия. Это развитие шло за счет освоения нового рынка с существенным отставанием развития от других стран. Государство стало регулировать развитие информационного общества только в 2011 году. В результате позднего государственного регулирования значительная часть трафика российского сегмента сети Интернет носит трансграничный характер, даже если клиент и сервер находятся на территории России. Очевидно, что в таких условиях отказаться от трансграничного трафика невозможно, даже в условиях принятия Федерального закона от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации».

Невозможность жесткого технического запрета нежелательного трафика заставляет искать иные пути. При этом необходимо иметь в виду, что борьба должна осуществляться не только по направлению блокирования информации, но и по направлению выявления лиц, размещающих запрещенную информацию и по направлению выявления лиц, собирающих такую информацию. Как правило, эти лица используют косвенные запросы не только для обхода блокировок сайта, но и для скрытия собственной личности, в частности, физического месторасположения.

Одним из возможных решений может являться компрометация средств выполнения косвенных запросов. Многие серверы хостинга предлагают своим клиентам услугу по защите от атак различного типа, в частности, от атак на отказ в обслуживании. Имитация такой атаки через известный VPN-сервис может повлечь срабатывание системы защиты и включение открытого VPN-сервиса в черный список. Таким образом, лицо собирающее или распространяющее информацию, оказывается перед невозможностью использования сервисов выполнения косвенных запросов.

Еще одним реализуемым решением может являться замедление VPN-трафика. Следует отметить, что публичные VPN-сервисы как правило по умолчанию имеют невысокую скорость, так что даже незначительное ее дальнейшее снижение может повлечь невозможность использования многих интернет–сервисов (потоковое видео, торренты и т. п.).

Ограничение VPN-трафика имеет целью сделать некомфортной анонимную работу с ресурсом. Однако, даже отказ от VPN не всегда позволяет установить реальные сетевые адреса участников обмена запрещенной к распространению информации. Злоумышленник может использовать для выхода в сеть Интернет и доступа к ресурсу публичные сети. В случае, если удалось выявить такую сеть с целью дальнейшего

установления личности злоумышленника можно воспользоваться стандартными уязвимостями информационных систем, в частности, организовать атаку типа «Evil Twin».

Атака «Evil Twin» является разновидностью MITM-атак и заключается в создании двойника точки доступа с тем же идентификатором. Если уровень сигнала двойника выше уровня сигнала точки оригинала, то в случае, когда устройство отслеживаемого злоумышленника подключается к сети автоматически, то подключение будет произведено именно к двойнику.

Если сайт с запрещенной информацией не имеет сертификата ключа шифрования, то использование двойника точки подключения позволяет собрать информацию о злоумышленнике.

В случае, когда сайт с запрещенной информацией имеет ключ шифрования, для сбора информации можно воспользоваться несовершенством сертификации. Все выдаваемые сертификаты разделяют на три уровня. При регистрации сертификатов первых двух уровней серьезной проверки заявителя не проводится, что дает возможность получить сертификат даже на юридическое лицо. Если наименование этого юридического лица будет близко к владельцу настоящего сайта, то наличие точки–двойника даст возможность по запросу переадресовать отслеживаемого злоумышленника на подконтрольный сайт-двойник в целях дальнейшего сбора информации.

В случае, когда известны какие-либо контактные данные отслеживаемого злоумышленника, можно провести так называемую XSS-атаку. Сущность такой атаки состоит в выполнении на атакуемом компьютере кода, расположенного на стороннем сервере.

Как правило, XSS-атаки проводятся с помощью специально–подготовленных ссылок. Активная атака при этом, скорее всего, будет невозможна, поскольку даже в случае наличия уязвимости на сайте, распространяющем запрещенную информацию, при активной атаке обязательно останутся следы на сервере провайдера хостинга. Однако, этот сайт можно использовать для пассивных атак методом «водопоя». Поскольку целью атак являются пользователи сайта с запрещенной информацией, то известна среда этих пользователей, и ссылки с XSS-атаками могут быть расположены на сайтах этой среды.

Конкретные цели атак определяются возможностями скриптовых языков. Наиболее распространенным языком является JavaScript, возможности которого, в частности, позволяют перехватить данные сессии или организовать атаку на отказ в обслуживании с целью компрометации сетевого адреса пользователя.

Перехват данных сессии позволяет получить авторизованный доступ к сайту с запрещенной к распространению информации. При отсутствии действий, направленных на загрузку информации, модификацию данных

пользователей такой доступ по умолчанию нельзя считать уголовным преступлением, поэтому XSS-атака может использоваться для выявления информации о лицах, поддерживающих распространение запрещенной информации и осуществляющих деструктивные действия в информационном пространстве Российской Федерации.

Перехват сессии также возможен в случае, если сайт с запрещенной информацией имеет уязвимость, связанную с некорректным управлением сессии. В частности, если сайт не использует в должной мере файлы cookie.

Резюмируя изложенное, следует отметить, что использование технических особенностей технологий, используемых при распространении информации через сеть Интернет, позволяет организовать внепроцессуальный сбор информации о лицах, поддерживающих распространение запрещенной информации, а также затруднить использование средств выполнения косвенных запросов. Однако, следует отметить, что такие действия, даже в рамках принуждения к исполнению законодательства, могут быть расценены, как преступное действие, поэтому в рамках совершенствования законодательства целесообразно рассмотрение вопроса о вводе таких действий в рамки закона.

Литература

1. Ивличев П.С., Ивличева Н.А. О принципах построения и использования имитационных моделей систем массового обслуживания в экономике // Евразийский юридический журнал. № 10. – 2018. – С. 452–455.

Ивличева Наталья Александровна,
psi940@mail.ru
Рязанский филиал
Московского университета МВД России
имени В.Я. Кикотя

ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: Статья посвящена перспективам реализации информационного суверенитета Российской Федерации

Ключевые слова: прокси-серверы, VPN-технологии, анонимные сети.

Регулирование информационных правоотношений началось в Российской Федерации с 1995 года с вводом в действие Федерального закона от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации». Данный закон был разработан и введен в действие в период, в который доступ к сети Интернет не был массовым. С развитием доступности сети закон довольно быстро стал бессмысленным, поскольку регулирование информационных правоотношений в законе было прописано довольно формально.

Развитие информационного права в Российской Федерации привело к появлению Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в котором уже изначально ряд сетевых определений был введен в правовое поле. В этом законе впервые появилось понятие запрещенной к распространению информации, к которой была отнесена информация которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иная информация, за распространение которой предусмотрена уголовная или административная ответственность.

Несмотря на то, что информационное законодательство с 2006 ввело Интернет в правовое поле, споры об эффективности такого регулирования идут до сих пор. Наличие формального запрета и даже угроза привлечения к ответственности далеко не всегда останавливают злоумышленников. Кроме того, охват информации в сети Интернет намного шире, чем при использовании традиционных источников, а возможность удаления информации, попавшей в сеть, оценивается крайне низко.

Новеллы концепции информационного суверенитета в Российском законодательстве начинают появляться в 2012 году, когда с юридической точки зрения начинают формулироваться определения понятий, специфических для сети Интернет (в частности, понятие сайта, страницы сайта, провайдера хостинга, электронного сообщения).

Неизбежность появления информационного суверенитета в Российской Федерации достаточно очевидна, поскольку в современном постиндустриальном обществе возможность государства самостоятельно определять порядок распространения информации на своей территории является необходимым атрибутом суверенного государства.

Принципы оборота информации, сформулированные в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» не дают возможности установить на территории России идеологический суверенитет, таким образом, изначально, суверенитет России в информационном поле носит технический характер.

Развитие технического суверенитета подразумевает наличие на территории страны информационных ресурсов различного плана (социальные сети, мессенджеры, форумы, новостные сайты, торрент-трекеры и т. п.), которыми пользуется значительная часть населения страны. Наличие таких ресурсов позволяет реализовать так называемую мягкую концепцию информационного суверенитета, поскольку в данном случае можно ограничить трансграничную передачу информации без нанесения серьезного ущерба привычным интересам пользователей национального сегмента сети Интернет.

Однако, помимо создания национальных ресурсов, концепция информационного суверенитета подразумевает контроль над размещаемой информацией, основной целью которого является обеспечение информационного спокойствия граждан. Информационное спокойствие особенно важно для противодействия информационным вбросам экстремистского толка, поскольку такие вбросы, как правило, ярко эмоционально окрашены и способны быстро создать в сознании потребителя информации яркий образ, который при преобладании клипового мышления становится руководством к деструктивным действиям.

Принимая во внимание тот факт, что большинство людей 1985 года рождения и моложе на территории России можно отнести к так называемым «цифровым аборигенам», для которых клиповое мышление является необходимым защитным механизмом от чрезмерного потока информации в сети Интернет, следует признать, что контроль размещаемой в сети информации является важной задачей, которую необходимо решить для борьбы с экстремизмом.

В связи с этим в рамках установления информационного суверенитет в 2012 году появилась единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

По замыслу законодателей, в случае обнаружения размещения запрещенной к распространению информации, оператор реестра должен уведомить провайдера хостинга, который, в свою очередь, должен уведомить о нарушении владельца сайта, на чьей странице размещена запрещенная к распространению информация. Обязанность удаления информации в этом случае ложится на владельца сайта. В случае непринятия владельцем сайта мер по удалению информации, ограничить доступ к сайту должен провайдер хостинга. Если же провайдер хостинга не принял мер по ограничению доступа к сайту, то сайт попадает в реестр. Доступ к сайтам из реестра ограничивается на уровне провайдеров услуг связи.

Разрабатывая порядок взаимодействия и контроля, законодатель, в первую очередь, решал юридические аспекты. Это связано с тем, что регулирование оборота информации может противоречить концепции режима свободного оборота информации, установленным Конституцией Российской Федерации. Кроме того, провайдер хостинга и владелец сайта связаны гражданскими правоотношениями и нарушение условий договора провайдером хостинга может стать основанием для иска со стороны владельца сайта. Кроме того, владелец сайта может размещать на своих страницах не только принадлежащую ему информацию, но и иную информацию, по договорам с третьими лицами. Удаление владельцем сайта такой информации также может стать основанием для гражданских исков.

С целью оградить провайдеров хостинга от таких исков, в 17 статью Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» было внесено дополнение, исключающее ответственность этих лиц при удалении или ограничении доступа к информации, распространяемой с нарушением закона.

Однако, реализация информационного суверенитета в сфере контроля над распространением информации экстремистского характера имеет ряд проблем, связанных как с организационными, так и с техническими проблемами.

Организационные проблемы борьбы с распространением экстремистской информации связаны с особенностями функционирования сети Интернет и его трансграничностью.

Исходя из смысла статьи 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» удалять информацию должен владелец сайта. Однако в случае, если информация носит заведомо экстремистский характер, о чем владелец сайта, разумеется, осведомлен, рассчитывать на его добросовестность не приходится. Кроме того, прекрасно понимая наличие потенциальных претензий со стороны России, владелец сайта постарается

осложнить процедуру блокирования контента. Сайт экстремистского содержания будет размещен у зарубежного провайдера хостинга. Рассчитывать на соблюдение российского законодательства зарубежными хостингами не приходится в силу разных причин. Это и текущая международная ситуация, и стремление заработать на любом контенте, и, возможно, прямой интерес зарубежных спецслужб.

К тому же, рынок хостинга довольно сильно развит, так что даже прекращение провайдером хостинга доступа к сайту приведет к тому, что владелец сайта просто поменяет провайдера хостинга. При этом, поскольку сайт сохраняет доменное имя, то для потребителей информации такой переезд окажется практически незаметным. Следует отметить, что блокирование сетевого адреса означает, фактически, блокирование всего хостинга. Однако, провайдеров хостинга такое развитие событий не пугает, поскольку у зарубежного сайта доля российских пользователей не велика.

Таким образом, с организационной точки зрения наиболее эффективным является включение сайта в реестр и запрет доступа на уровне российских провайдеров.

Однако, такое организационное решение не решает технических проблем запрета доступа. Технические проблемы связаны с простотой организации косвенных запросов к сайтам в сети Интернет. Для реализации таких запросов могут использоваться прокси-серверы, VPN-технологии, анонимные сети.

Тем не менее, функционирование реестра нельзя признать полностью провальным. За счет запрета доступа к страницам сайта, падает количество посещений, как следствие, снижаются расценки на размещение рекламы и общая рекламная выручка. Однако, следует иметь в виду, что организации экстремистского толка не ставят экономический успех основной целью, нередко они вообще не участвуют в реферальных программах, существую на деньги теневых спонсоров. В связи с этим, очевидно, что для неформального подхода к информационному суверенитету Российской Федерации потребуется разработка иных мер по контролю за распространяемой информацией.

Перспективными направлениями могут являться следующие:

1. Развитие технологий глубокого анализа пакетов информации. В данном случае можно отслеживать конечных потребителей информации экстремистского содержания или уничтожать пакеты в процессе их передачи.

2. Правовое и техническое регулирование использования VPN-технологий. В условиях широкого применения дистанционных технологий во многих сферах полный запрет на виртуальные частные сети невозможен и нецелесообразен. Однако, использование VPN для физических лиц можно ограничить. Отслеживание VPN-трафика также

можно осуществлять с помощью технологии глубокого анализа пакетов информации.

3. Развитие автономности российского сегмента сети Интернет и приоритет российского трафика над трансграничным.

Литература

1. Ивличев П.С., Ивличева Н.А. О принципах построения и использования имитационных моделей систем массового обслуживания в экономике // Евразийский юридический журнал. № 10. – 2018. – С. 452–455.

Катенко Юлия Викторовна,
yukatenko@baltinfocom.ru
ООО «БалтИнфоКом»

ПРИМЕНЕНИЕ АЛГОРИТМОВ КЛАССИФИКАЦИИ ДЛЯ ВЫЯВЛЕНИЯ ТЕКСТОВ ТЕРРОРИСТИЧЕСКОЙ ТЕМАТИКИ

Сегодня интернет является важнейшим каналом распространения информации. Являясь очень удобным и полезным инструментом для взаимодействия между людьми, интернет также активно используется злоумышленниками для различных преступных целей, таких как мошенничество, торговля наркотиками и пропаганда терроризма. Методы машинного обучения дают возможность автоматизировать поиск неправомерной и опасной информации в интернете и, в частности, в социальных сетях.

Машинное обучение – это научная область, находящаяся на пересечении статистики, искусственного интеллекта и компьютерных наук и также известная как прогнозная аналитика или статистическое обучение. Использование алгоритмов машинного обучения позволяет извлекать знания из данных без ручного построения жестких правил принятия решений. [1]

Задача классификации объектов – задача, в которой определено конечное множество объектов, каждый из которых относится к некоторой категории (классу), и необходимо построить алгоритм, способный определить, к какому классу относится произвольный объект. В данной работе решалась задача бинарной классификации, то есть разделения текстов на два класса: связанные и не связанные с тематикой терроризма.

Подготовка выборки для обучения

Для обучения модели бинарной классификации текстов необходима размеченная выборка, включающая тексты двух классов: «positive», то есть соответствующие выбранной тематике, и «negative» – не соответствующие.

Для создания набора текстов с меткой «positive» выполнялся поиск в социальных сетях и на различных сайтах, по ключевым словам, «терроризм», «теракт», «джихад», «моджахед» и др., по названиям известных террористических организаций и именам террористов.

Для получения текстов с меткой «negative» были загружены записи из сообществ в социальных сетях, имеющих различную тематику. Среди этих записей встречаются в том числе содержащие информацию о боевых действиях, оружии, различных катастрофах, то есть, лексически они могут быть близки с текстами о терроризме.

Выборки были дополнительно проверены вручную, чтобы исключить попадание текстов одного класса в подмножество текстов другого класса. Длинные тексты были разделены на несколько частей. В итоге была получена сбалансированная выборка, включающая более полутора тысяч текстов.

Модель классификации BERT

В качестве алгоритма для анализа текстов была выбрана модель BERT (Bidirectional Encoder Representations from Transformers) – нейронная сеть, разработанная специалистами Google и показывающая высокую производительность на различных задачах обработки естественного языка. Модель BERT предназначена для представления текстов в векторном виде. Добавив к этой нейронной сети дополнительный выходной слой и обучив на собственном наборе данных, можно создавать модели для решения широкого ряда задач, таких как классификация текстов или построение вопросно-ответных систем. [2]

Предобучение BERT состоит из двух этапов:

1. Предсказание замаскированных слов – в корпусе текстов, используемых для обучения, маскируется определенный процент случайно выбранных слов, и задачей модели является предсказание замаскированных слов на основании того, какие слова стоят справа и слева от них, то есть на их контексте.

2. Определение связей между предложениями – на вход модели подается два предложения, и ее задача – предсказать, является ли второе предложение продолжением первого или это случайное предложение из набора обучающих текстов.

Применение такого подхода к обучению и использование очень объемных корпусов текстов, например, статей из Википедии на выбранном языке, позволяет получить модель для векторного представления текстов с учетом контекста входящих в них слов.

В данной работе для извлечения векторных представлений использовалась предобученная многоязычная модель DistilBERT, облегченная и имеющая более высокую скорость работы по сравнению с классической моделью BERT. Дистилляцией знаний называется способ сжатия, когда небольшая модель обучается воспроизводить поведение большой и более медленной модели. [3, 4]

Для решения задачи классификации текстов к DistilBERT был добавлен полносвязный слой, и полученная модель была обучена на ранее описанной выборке. Оценка качества модели приведена в таблице 1.

Таблица 1

Оценка качества модели классификации текстов на связанные и не связанные с террористической тематикой

	Обучающая выборка			Проверочная выборка		
Точность (accuracy)	1.00			0.94		
Точность (precision)	1.00			0.94		
Полнота	1.00			0.94		
F_1–мера	1.00			0.94		
Матрица несоответствий		0	1		0	1
	0	2867	3	0	399	16
	1	19	2873	1	33	368

Оценка тональности текста

Авторы текстов на тему терроризма могут по–разному относиться к этому явлению (положительно, отрицательно или нейтрально описывать ситуацию), оценить это можно с помощью анализа тональности. Тональность текста – это выраженное в тексте эмоциональное мнение относительно некоторого объекта (объектов). Тональность можно измерять при помощи шкалы в диапазоне от положительного отношения до отрицательного. [5] Для решения задачи оценки тональности использовалась та же модель, что и для предыдущей задачи, но обученная на наборе текстов новостей, помеченных как имеющие положительную или отрицательную тональность. [6] Оценка качества модели определения тональности приведена в таблице 2.

Таблица 2

Оценка качества модели определения тональности текста

	Обучающая выборка			Проверочная выборка		
Точность (accuracy)	0.97			0.86		
Точность (precision)	0.98			0.86		
Полнота	0.97			0.86		
F_1–мера	0.97			0.86		
Матрица несоответствий		0	1		0	1
	0	16116	784	0	1928	465
	1	80	16830	1	221	2168

Модели, созданные в ходе данной работы, могут быть использованы для автоматизации анализа больших множеств текстов, которые невозможно обрабатывать вручную.

Поскольку в работе использовались только данные, полученные из открытых источников, модель классификации текстов на связанные и не связанные с террористической тематикой может неверно определять класс текстов, содержащих специфическую лексику, не представленную в обучающей выборке. Модель может быть дополнительно обучена, к примеру, с использованием текстов из закрытых сообществ в социальных сетях, где общаются участники террористических организаций, что повысит полноту классификации.

Литература

1. DistilBERT base multilingual model (cased) // Hugging Face. URL: https://huggingface.co/distilbert-base-multilingual-cased (дата обращения: 15.04.2021).
2. Jacob Devlin, Ming-Wei Chang, Kenton Lee, Kristina Toutanova. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1. 2019. URL: https://www.aclweb.org/anthology/N19-1423 (дата обращения: 15.04.2021).
3. Sentiment Analysis in Russian. Determine sentiments (positive, negative or neutral) of news in russian language. // Kaggle URL: https://www.kaggle.com/c/sentiment-analysis-in-russian (дата обращения: 15.04.2021).
4. Victor Sanh, Lysandre Debut, Julien Chaumond, Thomas Wolf. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter. URL: https://arxiv.org/abs/1910.01108 (дата обращения: 15.04.2021).
5. Андреас Мюллер, Сара Гвидо. Введение в машинное обучение с помощью Python. Руководство для специалистов по работе с данными – Вильямс, 2017. – 480 с.
6. Котельников Е.В. Комбинированный метод автоматического определения тональности текста // Программные продукты и системы. 2012. № 3. URL: https://cyberleninka.ru/article/n/kombinirovannyy-metod-avtomaticheskogo-opredeleniya-tonalnosti-teksta (дата обращения: 15.04.2021).

Котляр Анастасия Ильдаровна,
mvdlaw@yandex.ru
Крымский филиал
Краснодарского университета МВД России

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ БОРЬБЫ С ПРОЯВЛЕНИЯМИ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Проблемы использования сети интернет с целью пропаганды экстремистских идей в настоящее время являются предметом рассмотрения многих ученых. Высока актуальность недостатков функционирования механизмов, благодаря которым эффективно должны реализовываться имеющиеся способы профилактики экстремистской идеологии в нашей стране.

В сфере обеспечения государственной безопасности и противодействию экстремизма роль интернета возрастает с каждым годом. Это происходит в связи с массовым распространением информационных ресурсов среди населения всех возрастов и социальных групп, увеличением количества социальных сетей и их востребованностью. В особенности это актуально для подростковой социальной группы, у которых высока степень доверия к информационным ресурсам, из-за несформированности правильной модели мировоззрения такой категории лиц, им свойственна быстрая перемена взглядов и возможность осуществления на них влияния.

Глобализация информационных интернет ресурсов привела к охвату практически всех сфер деятельности, что, преимущественно, является положительной тенденцией. Однако достаточно велик риск распространения в сети деструктивной информации в сфере экстремизма и терроризма, что в настоящее время является проблемой общемирового масштаба. Современный киберэкстремизм способен продуцировать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой.

Наиболее остро проблема обеспечения информационной безопасности как составляющей национальной безопасности государства встает в контексте проявления транснациональной киберпреступности и кибертер-тероризма. При этом, угроза кибератак является вполне реальной, и связанные с ней риски оцениваются специалистами как высокие.

Одной из основных задач государства является борьба с проявлениями экстремизма, в том числе в интернет среде, что наиболее эффективно возможно осуществить путем внедрения инновационных технических средств. Для предупреждения и профилактики преступности экстремистской направленности регулярно принимается ряд мер,

развивается законодательство в данной сфере, разрабатываются новые информационно-телекоммуникационные средства. Кроме этого, посредством использования различных методов осуществляется формирование общего сознания нетерпимости у населения к проявлению экстремизма, уделяется особое внимание информационно не защищенной молодежной среде.

Для проявления экстремистской деятельности в сети интернет имеются благоприятные условия, что подтверждается количеством преступлений и административных правонарушений, совершаемых через ресурс, которое растет каждый год. К сожалению, государственный контроль в данной области не приносит ожидаемый эффект, большое число граждан нашей страны становятся жертвами экстремистов, орудующих во «всемирной паутине».

Основную деятельность по борьбе с экстремизмом осуществляет ряд правоохранительных органов, в большей степени Министерство внутренних дел Российской Федерации и Федеральная служба безопасности Российской Федерации. Иные органы власти и общественные объединения осуществляют профилактику экстремизма в той или иной части. По мнению некоторых ученных государственное управление ослаблено или полностью парализовано, объективно не способно системно и последовательно противостоять нарастающему экстремизму и терроризму. Органам власти требуется больше времени, определенных усилий и условий для выработки и принятия решений на законодательном и организационно-управленческом уровнях. С данной позицией мы согласны, так как проявления экстремизма, как в нашей стране, так и во всем мире, стремительно реформируются, меняют свою форму и содержание, в связи с чем, органы государственной власти не успевают принимать работающие меры противодействия.

Кроме того, является весомой поддержка общественности в данном направлении, так факты выявления экстремистского контента обычными пользователями, своевременная передача информации в уполномоченные органы и соответствующая реакция на это, позволяет предотвратить общественно-опасные последствия некоторой части противозаконных проявлений экстремизма.

Имеющиеся проблемы борьбы с интернет экстремизмом обосновываются многочисленными факторами, которые тяжело, а иногда невозможно преодолеть. В основном, это масштабность и изменчивость глобальной сети, проблемы идентификации пользователей, ограниченность профессионального ресурса, осуществляющего профилактику экстремизма и другие.

С целью повышения эффективности борьбы с экстремизмом определенными учеными предлагается провести разработку доктрины национальной безопасности Российской Федерации, которая послужит

основанием для разработки стратегий по отдельным направлениям, в соответствие с которыми должно быть приведено законодательство. В настоящее время в стране имеется ряд нормативно-правовых актов, содержащих нормы, обеспечивающие борьбу с распространением экстремизма, такие как Конституция Российской Федерации, Федеральные законы, Уголовный кодекс и Кодекс об административных правонарушениях российской Федерации, международные и подзаконные акты. Разработка такого рода доктрины будет являться правовой основой противодействия экстремистской деятельности на территории нашего государства.

Некоторые авторы считают целесообразным перенимать методы противодействия экстремизму, предпринимаемые некоторыми странами мирового сообщества, с чем мы солидарны. Так, за рубежом подтверждена эффективность создания при участии компаний, предоставляющих услуги в глобальной сети, наблюдательных советов и «горячих линий», которые имеют право оперативно удалять из сети Интернет материалы, имеющие экстремистскую и террористическую направленности. Данные меры являются действенными и необходимы к повсеместному внедрению в интернет ресурсе Российской Федерации.

В более глобальном контексте рассмотрения проблем противодействия экстремизма актуальным является мнение о необходимости активизирования межгосударственного сотрудничества и формирования общей международной нормативно-правовой базы в сфере регулирования данной группы правоотношений.

Задача противодействия экстремистским проявлениям в сети интернет является одной из первостепенных для Российской Федерации. Для борьбы с этим явлением принимаются всесторонние меры в разных сферах жизни, однако, они не всегда способны справляться с таким общественно опасным, массовым, быстро распространяющимся и изменяющимся явлением. Имеющиеся проблемы требуют дальнейшего изучения и выработки действенным мер по их разрешению.

Литература

1. Кипров И.А. Актуальные вопросы реформирования государственного управления российской федерации в области борьбы с экстремизмом и терроризмом // Актуальные проблемы гуманитарных и естественных наук. № 12-3. – 2016. – С. 56–59.

Кубасов Игорь Анатольевич,
ikubasov@mvd.ru
Академии управления МВД России

Минаев Александр Васильевич,
am3172@yandex.ru
ФКУ «ГИАЦ» МВД России

АСПЕКТЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОФИЛАКТИКИ РАДИКАЛИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Как известно: кто владеет информацией, тот владеет и миром. В этой парадигме борьбы за овладение миром можно выделить два аспекта: борьба за овладением достоверной, полной и своевременной информации, с одной стороны, и борьба за овладением умами потребителей путем «навязывания» им своей достоверной информации, с другой стороны. В силу этого многочисленные средства массовой информации, круглосуточно производящие бесконечные потоки информации по различным темам, иногда практически не оставляют неподготовленному потребителю возможности узнать достоверный информационный факт и сформировать свое отношение к произошедшему событию. Над информационным восприятием потребителя в целях завладения их умами работают без устали все средства. Их много, и все они разные. А по сему, нельзя здесь исключать навязанную тенденциозную, а порой и просто не достоверную информацию. Дело в том, что нейронные системы человека так устроены, что реакция на фальшивый образ и иную яркую недостоверную информацию является такой же, как если бы она была истиной. Особенно это характерно, когда выверенная под пользователя информация цепляет и удерживает в нем сильные эмоциональные ассоциации, доводящие порой до бессознательного состояния.

Имеется много примеров успешного информационного воздействия на молодежь. Молодежь в силу ряда факторов является социальной группой, которая наиболее восприимчива к радикально–националистическим и ксенофобским идеям и настроениям. Радикализм может проявляться в различных формах экстремизма и терроризма. При этом радикализм может быть исключительно «идейным», а не действенным, в отличие от экстремизма, который всегда бывает действенным, но не всегда идейным. Но в любом случае, молодежный радикализм – это генератор политической нестабильности, политического деструктивизма, перехода к несистемным формам политической активности молодежи [1, 2].

Игнорирование молодежного радикализма или применение карательных мер не дает положительного эффекта, необходим системный подход, направленный на купирование и минимизацию всех экономических, политических, социоструктурных и идеологических факторов, детерминирующих радикализацию молодежи.

В этой связи актуальным и важным является реализация комплекса мероприятий по профилактике молодежного радикализма, и в частности, применение современных технологий искусственного интеллекта (далее – ТИИ) для этих целей [3]. Это обусловлено тем, что именно данная категория населения, активно используя в своей повседневной деятельности современные технические устройства, является одним из самых массовых потребителей информационного ресурса Интернета. Следует отметить и обязательно учитывать возрастные особенности подрастающего поколения:

– порой полное, чаще частичное, отсутствие идеологически сформированного современного подросткового и молодежного сознания;

– практически отсутствие некоторых нравственных ориентиров;

– легкая возбудимость в силу подростковой эмоциональности.

Эти и многие другие особенности подросткового сознания, отличающегося легкой и быстрой внушаемостью, позволяют посредством тенденциозного информационного воздействия перепрограммировать поведение подрастающего поколения.

Следовательно, в развязанной гибридной информационной войне молодежь – первостепенная мишень. Над завладением умами и эмоциями молодежной аудитории работает без устали циничный конвейер, основанный на интеллекте естественном, а в последнее время, не без успеха, активно привлекающий свою бездушную искусственную производную – интеллект искусственный (далее – ИИ). Колоссальные объемы информации, скорость их обработки и передачи ранее не имели таких показателей. Это изменение настолько впечатляющее, что за ним практически не успевает индивидуальное восприятие. Все это ведет напрямую к нарастанию информационного хаоса, своеобразному смешению миров: мира реального и мира виртуального. И в этом «информационном реакторе» расшатываются ранее сформированные, при социализме коллективные ценности, когда «раньше надо было думать о Родине, а потом о себе», сбиваются жизненные ориентиры, не соблюдаются действующие нормы поведения. На примере современной молодежи, как у нас в стране, так и в ближайшем зарубежье, сейчас именно это и наблюдаем [4].

Основной причиной социальной дезориентации, без сомнения, является информационный хаос, целенаправленно внедряемый враждебными СМИ различными способами. Заключается это в тенденциозной подаче неадекватной информации, а порой и просто

дезинформации. Выборочная подача фактов, их намеренное искажение подчиняется целям оголтелой пропаганды. Цели, которые преследуются при этом такие: у потребляющего этот информационный мусор должны возникать четкие, запланированные отправителем ассоциации.

Современный уровень развития информационных технологий и возможностей существующих систем ИИ позволяет выделить ряд принципиально новых угроз информационно-психологической безопасности молодежи. При этом скорость, с которой инакомыслие накапливается в Интернете, поражает воображение. Питательная среда – государственная идеология – резко сузилась, социальные сети, наплыв западных ценностей 80–90 годов дали свои разрушительные всходы. Начиная с 90 годов, враждебные информационные ресурсы породили идеологический разрыв. Исходя из этого, некоторая молодежь пытается самостоятельно отвечать на насущные вызовы современности, исследуя информацию доступными путями – в основном, сетями Интернет. Самореализация, основанная на неудовлетворенности своего положения, абстрагирующаяся от общества, ставящая личную выгоду выше выгоды коллективной выступает двигателем молодежного прогресса.

Одним из наиболее тревожных моментов данной ситуации является то, что молодежь столкнулась с тем, что, как некоторым кажется, есть возможность зарабатывать, не прикладывая труда. Так можно иметь много денег, не обладая профессией, занимаясь творческой работой в свободном графике, в свое удовольствие. Труд для них перестал быть тождественным заработку. И современных примеров тому, популяризированных СМИ, не счесть.

Здесь хочется вспомнить прусского военного теоретика и историка Карла Клаузевица: «Война – это акт насилия, имеющий целью заставить противника выполнить вашу волю». Анализируя сказанное выше, как мы ответим на вопрос: «Идет ли гибридная война на территории нашей страны? Есть ли промежуточные победы у противника в этой войне?». А если это изречение нацелить на перепрограммирование уже во многом зараженного молодежного сознания средствами ИИ, лишенных каких-либо человеческих эмоций, разработанных в странах агрессоров, тогда представляется возможным результат спрогнозировать заранее.

Анализируя средства, которыми могут влиять на радикализацию молодежной аудитории, прежде всего, следует отметить использование современных западных технологий «фальшивых людей» и «deep fake» для провокаций. Как рыбу на крючок цепляют молодежь, жаждущую перемен, «перемен которые требуют наши сердца», как звучит в словах кумира молодежи Виктора Цоя. Вот и вскрывается большая и циничная западня.

Американская технологическая компания «NVIDA» недавно поделилась результатами работы генеративно-конкурентной сети, обученной генерировать самостоятельно изображения несуществующих

людей, которая может добавлять любые культурные и этнические признаки. Использование такого рода ИИ для дестабилизации в обществе путем целевого высокотехнологического информационно-психологического воздействия на людей представляет очевидную и большую опасность. Однако угрозы непосредственно для информационно-психологической безопасности от радикализации взглядов молодежи до сих пор не были выделены в самостоятельную область рассмотрения.

При этом необходимо понимать, что все мы абсолютно прозрачны в цифровом пространстве. И это уже сейчас. Практически ничего не удается скрыть. Далеко не все готовы смириться с таким положением дел, но это ключевой вектор на ближайшие годы.

В этой связи представляется уместным объединить усилия оперативного состава, работающего по профилактике радикализма в молодежной среде, а также профессиональных психологов, аналитиков и программистов для разработки совместной теоретической и практической концепции борьбы за умы молодежи. В рамках разработки и внедрении данной концепции предлагается автоматизировать процесс сбора и обработки данных, как по результатам психологического тестирования, так и по результатам обработки информации в социальных сетях.

Таким образом, совместная работа по профилактике радикализма в молодежной среде может сводиться к следующему:

– создание материально-технической базы, способной осуществлять обработку больших объемов информации, морально-психологически характеризующих индивидуумов не статично, а во времени;

– разработка соответствующих психологических и математических моделей, способных на основе применения ТИИ заранее выявлять в социальных сетях и обществе того или иного индивидуума радикальных взглядов, при этом необходимо учитывать личные особенности отдельных молодых людей, временные наблюдения и поведение;

– административно-правовое регулирование в данной сфере общественных отношений.

Данные ТИИ должны позволять выявлять девиантное поведение и прогнозирование будущих действий объектов, подверженных радикализму [5,6]. Создаваемые экспертные автоматизированные системы (с участием оперативных сотрудников, специалистов-психологов и педагогов), основанные на заданных принципах, таких как способность к конкретизации и обобщению, совмещенность мыслительных действий ИИ и человека, позволят в режиме on-line наблюдать дистанционно за объектами, подверженными радикализму, анализировать полученную информацию, давать практические рекомендации, и, как следствие, заблаговременно пресекать противоправные действия.

Литература

1. Абрамов А.Э. Молодежный экстремизм как угроза национальной безопасности России в условиях глобализации. Общество: политика, экономика, право. 2020. № 5 (82). С. 52–55.

2. Кубасов И.А., Мельников А.В., Мальцев С.А., Нарушев И.Р. Кластеризация объектов со слабо формализуемыми признаками на основе нейронной сети в виде слоя Кохонена. Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 3 (77). С. 86–91.

3. Мухаметзарипов И.А., Гибадуллина М.Р. Применение визуальных материалов в профилактике агрессии и экстремизма среди молодежи: зарубежный и отечественный опыт. Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. 2019. № 4 (56). С. 146–153.

4. Нарушев И.Р., Мальцев С.А., Кубасов И.А. Численный метод сшивания объектовой базы экспертизы девиантного поведения несовершеннолетних при использовании метода анализа иерархий. Вестник Воронежского института ФСИН России. 2018. № 4. С. 89–97.

5. Салахова В.Б., Ерофеева М.А., Артамонова Е.Г. Правоприменительная практика органов исполнительной власти субъектов Российской Федерации по профилактике терроризма и экстремизма. Человеческий капитал. 2020. № 9 (141). С. 86–103.

6. Шапкин А.В., Кубасов И.А., Конюшев В.В. МВД России: дорога к искусственному интеллекту. В сборнике: Искусственный интеллект (большие данные) на службе полиции. Сборник статей международной научно–практической конференции (28 ноября 2019 г.), 2019. С. 236–243.

Кубасов Игорь Анатольевич,
ikubasov@mvd.ru
Академия управления МВД России

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Экстремизм и терроризм во всех формах проявлений выступают одним из основных факторов, дестабилизирующих устойчивое развитие любого общества, в том числе и российского. На современном этапе развития российского общества особую актуальность приобрели вопросы, связанные с определением роли и места инновационных технологий (прежде всего, информационно-телекоммуникационных технологий) в противодействии экстремизму и терроризму. Это обусловлено вступлением мирового сообщества в четвертую научно-техническую революцию, основным содержанием которой является глобальное развитие информационно-телекоммуникационных систем на основе перспективных информационных технологий и цифровых средств связи.

Важнейшим условием повышения эффективности борьбы с экстремизмом и терроризмом является широкое внедрение информационно-телекоммуникационных технологий, обеспечивающих получение более полной и своевременной информации о террористических структурах, об их планах по совершению террористических актов, деятельности по распространению идеологии терроризма и экстремизма. Правоохранительные органы постоянно ведут оперативно-аналитическую работу по получению информации об источниках и каналах финансирования террористически настроенных личностях и организациях, источниках снабжения их оружием, боеприпасами, иными средствами для осуществления террористической деятельности.

Эффективное противодействие экстремизму и терроризму возможно только путем реализации комплекса мероприятий, в ходе которых применяются различные формы и методы – взаимосвязанные и согласованные между собой технологии (в том числе, информационно-телекоммуникационные), приемы и средства воздействия на субъекты терроризма; купирование факторов, способствующих возникновению и развитию экстремизма и терроризма; минимизация (ликвидация) последствий террористических проявлений.

Осуществление борьбы с экстремизмом и терроризмом предполагает приоритетное использование методов выявления, предупреждения и пресечения террористической деятельности с целью адресного силового и психологического воздействия на конкретные субъекты терроризма. Борьба с терроризмом осуществляется также в форме различных оперативно-боевых, оперативно-поисковых, оперативно-розыскных,

блокирующих, фильтрационных, правоприменительных и иных действий с целью выявления, пресечения, раскрытия и расследования преступлений террористического характера.

Очень значимой составляющей оперативно-розыскной деятельности является оперативная идентификация личностей, причастных к совершенным террористическим актам, и в частности по анализу ДНК, изъятых с мест преступлений.

Следовательно, информационно-телекоммуникационные технологии в противодействии экстремизму и терроризму целесообразно применять комплексно по основным трем направлениям:

в целях профилактики терроризма в ходе разъяснительно-предупредительной работы в борьбе с экстремистскими проявлениями, а также при осуществлении нормативно-методической деятельности антитеррористического содержания [1–4];

непосредственно в борьбе с терроризмом – при выявлении, предупреждении, пресечении, раскрытии и расследовании террористического акта и иных преступлений террористического характера [5–8];

для минимизации и (или) ликвидации последствий террористических актов [9, 10].

Следует отметить, что с учетом основных задач дальнейшего развития ИСОД МВД России, указанных в «Основных направлениях дальнейшего развития единой системы информационно–аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы» [11, 12], и мероприятий Ведомственной программы цифровой трансформации МВД России на период 2021–2023 годов [13], весьма актуальным является применение инновационных технологий анализа больших данных, искусственного интеллекта и методов биоинформатики для определения индивидуальных фенотипических признаков человека на основе анализа биологического материала, а также выявления признаков серийности (сходности) определенных категорий преступлений.

Так, одной из задач Ведомственной программы цифровой трансформации МВД России на период 2021–2023 гг. является ликвидация имеющихся отставаний по вопросам применения технологий искусственного интеллекта. Планируется получить следующие результаты применения инновационных технологий по выявлению признаков серийных преступлений:

повышение эффективности деятельности МВД России за счет улучшения показателей по выявлению, раскрытию и расследованию преступлений;

выявление скрытых закономерностей, влияющих на раскрытие однотипных преступлений в субъектах Российской Федерации;

повышение качества данных розыскных, оперативно-справочных и криминалистических учетов за счет возможности выявлять скрытые закономерности в различных не структурированных текстовых данных.

Применение инновационных технологий по определению индивидуальных фенотипических признаков человека, полученных из биологического материала с мест совершения преступления, должна обеспечить:

повышение показателей по розыску лиц (неопознанные труппы, психо-физический портрет преступника);

применение разработанных технологий при выявлении генетических аномалий и закономерностей;

экспорт готовых технологий в зарубежные страны в области криминалистического ДНК-анализа.

ДНК несет в себе набор генетических инструкций определяющих, в том числе и фенотипические признаки человека, вызывая широкий спектр их проявлений среди людей. Определив, как генетическая информация преобразуется в фенотипические признаки, можно «реконструировать» ДНК в физический профиль, предсказать, как выглядит неизвестный человек.

Таким образом, в отличие от традиционной экспертизы ДНК (образец неизвестной ДНК, полученный с места совершения преступления, сопоставляется с образцами ДНК известных подозреваемых или с базой данных ДНК), фенотипирование ДНК может дать новые сведения о человеке, даже если он ранее не был идентифицирован и сведения о ДНК отсутствуют в базе данных. Фенотипирование ДНК использует преимущества современной технологии SNP-маркеров для чтения частей генома, которые кодируют различия между людьми.

В настоящее время системы, разработанные зарубежными учеными на основе биоинформатики и технологий искусственного интеллекта, преобразуют информацию о SNP-маркерах из образца ДНК неизвестного лица в предсказание его происхождения и таких внешних черт, как цвет кожи, цвет волос, цвет глаз, наличие веснушек и даже морфология лица. Прогноз фенотипа делается с определенной вероятностью, в том числе, позволяя с высокой степенью вероятности исключать некоторые признаки. Например, точность того, что глаза зеленые 86,4%, и что они не коричневые 99,0%.

Однако известные зарубежные наработки мало или вообще не применимы для Союзного государства (Россия и Белоруссия), так как не дают необходимой точности. Это обусловлено привязкой аналитического аппарата технологий ДНК-идентификации к генетическим характеристикам населения конкретного региона. Для реализации такого подхода в рамках научно-технической программы Союзного государства «Разработка инновационных геногеографических и геномных технологий

идентификации личности и индивидуальных особенностей человека на основе изучения генофондов регионов Союзного государства» (НТП «ДНК-идентификация»), разработанной ФАНО России совместно с Национальной академией наук Республики Беларусь и рассчитанной на выполнение в 2017–2021 гг. (ответственным исполнителем Российской части программы является Институт общей генетики им Н.И. Вавилова РАН), создана база данных, содержащая характеристику генофондов 140 этнорегиональных групп населения России, Белоруссии и сопредельных стран. Генофонд каждой популяции охарактеризован по 4 млн. генетических маркеров. Разработаны технологии определения вероятного этногеографического и популяционного происхождения неизвестного индивида по его ДНК [14].

Разработанная технология ориентирована на характеристики генофондов населения российских регионов и позволяет предсказывать цвет глаз и волос по генетическим маркерам с точностью до 88% для светлого цвета радужки глаз, 90,20% – для темного цвета; 65,6% – для светлого цвета волос, 86,5% – для рыжих волос, 74% – для черных волос, 83% – для смешанного светло–темного оттенка волос.

В настоящее время разрабатывается технология определения вероятного возраста неизвестного индивидуума по ДНК. На данный момент точность предсказания возраста при исследовании образцов ДНК крови составляет 3,8 года, буккального эпителия (поверхностный слой клеток ткани внутренней полости рта) – 4,6 года, спермы – 2,7 года.

Разработаны методики оценки статуса курения и потребления алкоголя по прижизненной химической модификации ДНК индивида. Определены генетитические особенности людей с различным темпераментом, психикой. Появилась ДНК-технология, определяющая психоэмоциональный статус человека.

В результате дальнейших научно-исследовательских и опытно-конструкторских работ запланировано создание программных решений с последующим вводом в эксплуатацию новых сервисов ИСОД МВД России, востребованных подразделениями МВД России, не позднее 2024 года. При чем данные результаты представляют собой кросс-ведомственные решения, так как могут быть использованы без существенных доработок в деятельности Следственного комитета Российской Федерации, Прокуратуры Российской Федерации, ФСБ России, Росгвардии, ФСИН России.

Внедрение рассмотренных инновационных технологий в практику правоохранительных органов не только вооружит современными методами криминалистических исследований, но и будет способствовать повышению эффективности расходования бюджетных средств в противодействии экстремизму и терроризму.

Литература

1. Ведомственная программа цифровой трансформации МВД России на период 2021–2023 годов, утвержденная Распоряжением МВД России №1/15065 от 29.12.2020.
2. Дедков В.К., Бобр О.А., Кубасов И.А. Вопросы синтеза безопасности объектов защиты. Стратегическая стабильность. 2006. № 2 (35). С. 45–50.
3. Кубасов И.А. Математическая модель оценки эффективности информационно–аналитического обеспечения подразделения в специальной операции. В сборнике: Состояние и перспективы развития современной науки по направлению «АСУ, информационно-телекоммуникационные системы»: сб. ст. II Всерос. науч.-тех. конф. Военный инновационный технополис «ЭРА». Анапа, 2020. С. 109–116.
4. Кубасов И.А. Методика категорирования потенциально опасных объектов по степени защищенности с применением логарифмической шкалы. Надежность и качество сложных систем. 2020. № 3 (31). С. 121–127.
5. Кубасов И.А. Обоснование показателя эффективности управления подразделением при осуществлении специальной операции. Информационные системы и технологии. 2020. № 1 (117). С. 71–76.
6. Кубасов И.А. Подходы к обоснованию требуемых значений показателей эффективности связи в специальной операции. Вестник Воронежского института МВД России. 2020. № 1. С. 116–124.
7. Кубасов И.А. Управление безопасностью потенциально опасных объектов. Надежность и качество сложных систем. 2020. № 4 (32). С. 42–49.
8. Кубасов И.А. Условия оптимального управления подразделением МВД России при осуществлении специальной операции. Вестник Воронежского института ФСИН России. 2019. № 3. С. 74–79.
9. Кубасов И.А., Мельников А.В., Мальцев С.А., Нарушев И.Р. Кластеризация объектов со слабо формализуемыми признаками на основе нейронной сети в виде слоя Кохонена. Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 3 (77). С. 86–91.
10. Кубасов И.А., Пучков Г.Ю. Анализ технических решений в области организации оперативной радиосвязи и особенности использования беспилотных летательных аппаратов в интересах органов внутренних дел российской федерации. Известия ЮФУ. Технические науки. 2012. № 3 (128). С. 41–48.
11. Нарушев И.Р., Мальцев С.А., Кубасов И.А. Численный метод сшивания объектовой базы экспертизы девиантного поведения несовершеннолетних при использовании метода анализа иерархий. Вестник Воронежского института ФСИН России. 2018. № 4. С. 89–97.

12. Научно-техническая программа союзного государства «Разработка инновационных геногеографичесих и геномных технологий идентификации личности и индивидуальных особенностей человека на основе изучения генофондов регионов Союзного государства» («ДНК-идентификация»), утверждена постановлением Совета Министров Союзного государства от 12 мая 2016 г. № 12 «О Концепции научно–технической программы Союзного государства "Разработка инновационных геногеографических и геномных технологий идентификации личности и индивидуальных особенностей человека на основе изучения генофондов регионов Союзного государства"».

13. Шапкин А.В., Кубасов И.А. Основные направления дальнейшего развития ИСОД МВД России на период с 2020 по 2024 годы. В сборнике: Стратегическое развитие системы МВД России: состояние, тенденции, перспективы. Сборник статей Международной научно–практической конференции. 2019. С. 254–259.

14. Шапкин А.В., Кубасов И.А., Конюшев В.В. МВД России: дорога к искусственному интеллекту. В сборнике: Искусственный интеллект (большие данные) на службе полиции: сб. ст. Междунар. науч.-практ. конф. (28 ноября 2019 г.), 2019. С. 236–243.

Кулибаба Николай Владимирович,
Краснодарский университет МВД России

Куропятник Дмитрий Леонидович,
Краснодарский университет МВД России

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Аннотация: В данной статье поднимается острая проблема, связанная с необходимостью поиска информационных и телекоммуникационных технологий, позволяющих в условиях глобальной цифровизации и зачастую бесконтрольности цифровых следов и больших данных, противостоять экстремистским и террористическим тенденциям современного социума

Ключевые слова: экстремизм, терроризм, кибертерроризм, информационная безопасность, защита информации, медиа-педагог

Введение. За последние десятилетия поток информации, то есть легкость и скорость, с которой информация проходит через общество, преобразился практически во всех странах, как никогда раньше. Эта

тенденция в решающей степени обусловлена коммуникационными технологиями (ИКТ) для облегчения и ускорения свободного потока информации. Особенности образования и рынка труда в цифровую эпоху, информационно-коммуникационные технологии в образовании, массовое применение информационно-коммуникационных технологий (ИКТ) радикально и всеобъемлюще трансформируют общество, процесс которого определяется как цифровая революция и используется в качестве инструмента для строительства глобального постиндустриального информационного общества.

Цифровая трансформация проявляет себя в массовой роботизации, внедрении -нано, -био, -инфо, -когно, -социо (НБИКС) технологий и их конвергенции с последующим изменением организации производства, обмена, потребления, социума, коммуникаций и конечно человека и его сознания (рис. 1.).

Рис. 1. НБИКС-технологии и их конвергенционная парадигма применения

Развитие технологий кардинально меняют рынок труда во всех отраслях и профессиях, в производственной сфере, продаже товаров и услуг, системе государственного управления и перестраивает кадровый потенциал, который по прогнозам футурологов за ближайшие 20 лет затронут до 70% рабочих мест. И сложность опережения этих технологий обусловливает качественную метаморфозу всего киберпространства в целом, и, в частности, мира киберпреступлений. Открываются все новые возможности для оттачивания «мастерства» киберпреступников.

Изложение основного материала статьи. Тема информационной безопасности с каждым днем все чаще выходит, как проблема в педагогической среде образовательных учреждений разного типа. Сейчас дети, с которыми мы работаем, студенты, подростки, – это поколение Z,

это люди, которые большую часть своего жизненного времени проводят в социальных сетях, и глобальной сети Интернет. Если мы обратимся к опросам общественного мнения, то придем к выводу, что количество молодых людей в возрасте 12+, погруженных в виртуальный мир социальных сетей неуклонно растет.

Каким же образом следует действовать педагогу, чтобы оградить подростков, молодых людей от необдуманных поступков и действий, что собой представляют экстремистские правонарушения в сети Интернет, что такое культура информационного общения, как правильно выражать свои мысли в сети Интернет, чтобы они не были двояко трактованы, т.к. это может привести к достаточно серьезным последствиям.

Если проанализировать концептуальные подходы, которые охватывают самую уязвимую для экстремистских и террористических преступлений целевую аудиторию, то это, безусловно, педагоги. Нынешний педагог должен идти в ногу со временем, он должен быть медиа-педагогом, человеком, который не просто может сформировать у своих студентов, школьников так называемые «soft-skills» (мягкие навыки), но и привить им возможность работать в команде, развивать свою мотивацию, но это, прежде всего, человек, который глубоко погружен в цифровую среду.

Это тот человек, который активно пользуется социальными сетями, знает, что в них происходит, знает, все эти изменения и тенденции. Наша главная задача – предупреждать, а не предотвращать серьезные последствия тех или иных прецедентов. Так, например, Фонд Общественного мнения, опубликовал следующие данные: в ходе исследований: родительскую общественность спросили: «Кто несет ответственность за безопасность детей в сети Интернет?» 78% респондентов возлагают ответственность на родителей, 52% опрошенных считают ответственными за это владельцев сайтов и различных приложений в сети Интернет, 42% ответов пришлось на государственные органы, осуществляющие надзор в сфере Интернет, и 13% возлагают ответственность, прежде всего, на школу, образовательные организации, педагогов, 12% респондентов возлагают ответственность на самих детей.

На вопрос: «Пользуетесь ли Вы интернетом, если «да», то как часто?» был проведен закрытый опрос среди свыше полутора тысяч человек, и оказалось, что за 10 лет процент пользования Интернетом и социальными сетями вырос практически в 20 раз. В России количество интернет-пользователей, по данным Digital 2020, составило 118 миллионов. Это 81% россиян. Соответственно, очевиден прирост и преступлений информационного характера.

Рис. 2. Количественные и процентные показатели динамики применения средств воздействия в войнах и вооруженных конфликтах, колич. %

Как видно из диаграммы (рис. 2), специалисты по ведению информационных войн подчеркивают, что по критерию эффективность-стоимость информационно-психологические и информационно-технические средства и технологии воздействия на противника существенно превосходят воздействия, осуществляемые с применением обычных систем и средств вооружения.

В ходе анализа официальной статистики количества приговоров по экстремистским статьям Уголовного кодекса РФ была сформирована диаграмма, иллюстрирующая данный показатель в ретроспективной динамике с 2007 года по настоящее время (рис. 3).

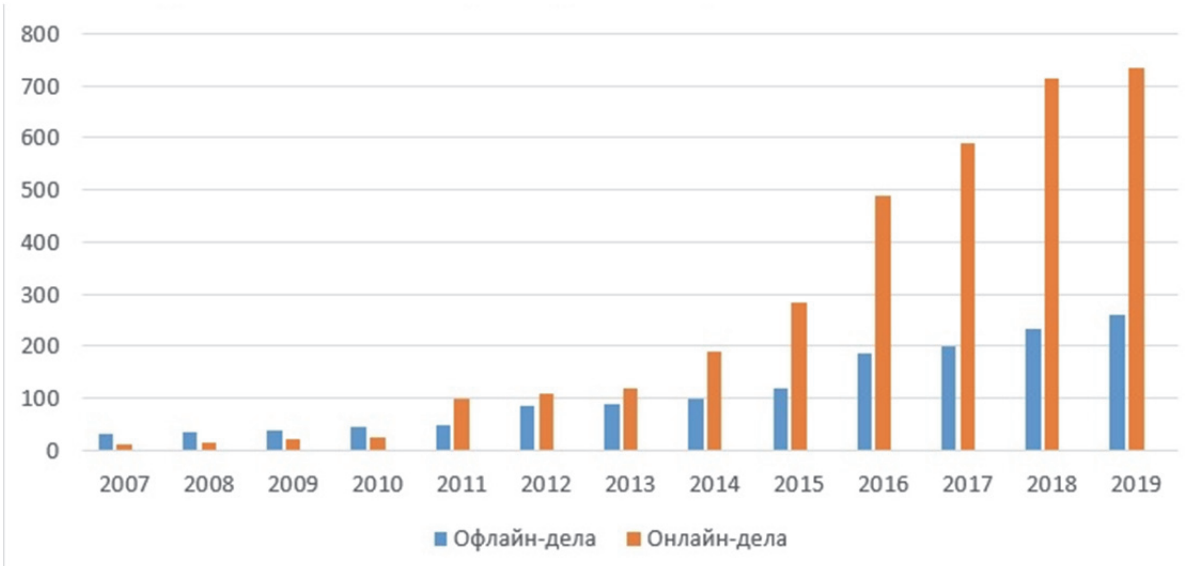


Рис. 3. Динамика количества приговоров по экстремистским статьям УК РФ в период с 2007 по 2019 гг.

В своей статье «Информационное обеспечение противодействия экстремизму» Скребец Е.С. делает акцент на изменении сущностной характеристики современного экстремизма, которая проявляется в его колоссальных возможностях к «…видоизменению, преобразованию и выработке новых форм, методов и путей осуществления деятельности». Поэтому противодействие экстремизму должно начинаться с разъяснения понятия и сущности экстремизма, его тягчайшего инерционного влияния на социум и государство.

Выводы. Методы эффективной обработки, хранения, анализа и использования информации – это одна из самых молодых технологий середины прошлого и начала XXI века, без которой невозможно представить жизнь современного человека (Интернет, мобильные телефоны и другое). Сегодня необходимо оказывать такого рода воздействие на граждан, которое видит своей целью воспитание у них отрицания идеологии насилия, в качестве ресурса может выступать и привлечение их к участию в противодействии экстремизму.

Литература

1. Официальный сайт Судебного Департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru (дата обращения: 25.03.2021).

2. Братусин А.Р., Скобликов Р.В., Кашин О.В. О необходимости подготовки на базе вузов МВД и силовых ведомств РФ специалистов в области информационной безопасности // Проблемы современного педагогического образования. 2019. № 63-4. С. 27–31.

3. Братусин А.Р. Проблема кибертерроризма как многоаспектный феномен технологических и политических реалий современного мира // Проблемы современного педагогического образования. 2018. № 60-4. С. 65–67.

4. Скребец Е.С. Информационное обеспечение противодействия экстремизму // Вестник КРУ МВД России. 2015. № 4 (30). URL: https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-protivodeystviya-ekstremizmu (дата обращения: 25.03.2021).

Лекарь Людмила Антоновна,
Научно-производственное объединение
«Специальная техника и связь»
Министерства внутренних дел Российской Федерации

Калугин Алексей Валерьевич,
alvakalugin@mvd.ru
Научно-производственное объединение
«Специальная техника и связь»
Министерства внутренних дел Российской Федерации

Карбова Елена Сергеевна,
elkarbova@yandex.ru
МИРЭА – Российский технологический университет

Калугин Дмитрий Алексеевич,
kalugin.d27o@gmail.com
МИРЭА – Российский технологический университет

БЕЗОПАСНОСТЬ УМНЫХ УСТРОЙСТВ: УГРОЗЫ И ВОЗМОЖНЫЕ РЕШЕНИЯ

Аннотация: Интеллектуальная сеть (ИС) – способ организации системы передачи информации, ориентированной на предоставление услуг и управление ими, при этом ИС занимает одно из самых важных приложений Интернета вещей (IoT). Развитие и применение информационных и коммуникационных технологий в традиционных энергосистемах, также обуславливает развитие киберфизических систем умных сетей. Системы интеллектуальных сетей на основе Интернета вещей являются критически важными инфраструктурами, также они имеют сложную архитектуру и включают в себя критически важные устройства. Нарушения работы интеллектуальной сети могут нанести ущерб национальной безопасности, привести к нарушению общественного порядка, гибели людей или крупномасштабному экономическому ущербу, когда нарушается конфиденциальность, целостность или доступность связи. Такие масштабные системы могут быть уязвимы для кибератак.

Интернет вещей (англ. Internet of things, IoT) – это концепция сети передачи информации между «умными» устройствами. Внутри IoT люди могут общаться с «вещами», а «вещи» – общаться между собой. Интернет вещей означает подключение различных устройств через Интернет или решения на основе IP. Устройством может быть что угодно: холодильник, датчик, кондиционер, мобильный телефон, автомобиль, персональный

компьютер или ноутбук. Устройства могут быть подключены через не-IP решения в небольшом масштабе. IoT также нацелен на крупномасштабное соединение всех видов устройств через IP-решения. В сети IoT устройства могут взаимодействовать или обмениваться данными напрямую или через шлюз по IP-адресам через Интернет.

В настоящее время существует много IoT-приложений, например: мониторинг загрязнения, умные дома и города, интеллектуальные автомобили. Но самым крупным приложением Интернета вещей является интеллектуальная сеть (ИТ). Система интеллектуальной сети, от производства энергии до потребителя, оснащена двунаправленными интеллектуальными устройствами, такими как датчики, исполнительные механизмы и интеллектуальные счетчики, что позволяет обеспечивать баланс, мониторинг и контроль в реальном времени в любом месте и в любое время с высокой степенью детализации и точности.

IoT – приложения очень удобно использовать для «умных» систем, но в них возможны уязвимости, которые могут привести к сбою или отказу системы. Так как контроль и мониторинг осуществляются с помощью интернет-протоколов и общедоступных решений, интеллектуальная сеть достаточна привлекательна для злоумышленников как критически важная инфраструктура. Например, злоумышленник может атаковать электрические устройства, нарушив баланс в реальном времени между производством и потреблением энергии из-за искажения данных, созданных устройствами [2]. Поэтому очень важно тщательно изучить компоненты и выявить существующие уязвимости и все возможные угрозы в инфраструктуре интеллектуальной сети.

Все системы должны быть спроектированы так, чтобы гарантировать защиту. В статье не рассматриваются меры необходимые для сертификации по уровням защиты информации в установленном порядке. В качестве обеспечения основы безопасности ИС рассматривается (триада сервисов) – конфиденциальность, целостность и доступность.

1. Безопасность в интеллектуальных сетях

Постоянное развитие информационных технологий содействует превращению традиционной электросети в интеллектуальную. Кибербезопастность является одним из ключевых критериев при разработке ИС. Проблемы с кибербезопасностью интеллектуальных сетей могут привести к значительному ущербу.

1.1. Основа безопасности ИТ-инфраструктуры

Основа безопасности ИТ-инфраструктуры интеллектуальной сети должна предусматривать меры, обеспечивающие защиту информации с помощью триады сервисов. Эти ключевые принципы безопасности должны обязательно соблюдаться в интеллектуальных сетевых системах.

Меры конфиденциальности защищают информацию от несанкционированного доступа и неправомерного использования.

Большинство информационных систем содержат информацию, имеющую некоторую степень конфиденциальности. Это может быть служебная, бизнес-информация, которую конкуренты (или злоумышленники) могут использовать в своих интересах, или личная информация о сотрудниках, клиентах. Конфиденциальная информация имеет ценность, и поэтому системы часто подвергаются атакам. Злоумышленники ищут уязвимости, чтобы воспользоваться ими. Векторы угроз включают, как прямые атаки, такие как кража паролей и перехват сетевого трафика, так и более многоуровневые атаки, такие как атаки с использованием социальной инженерии, например, фишинг. Не все нарушения конфиденциальности являются преднамеренными. Несколько типов распространенных случайных нарушений включают отправку конфиденциальной информации неправильному получателю по электронной почте, публикацию личных данных на общедоступных веб–серверах и отображение конфиденциальной информации на мониторе компьютера. В интеллектуальной сети могут быть домашние устройства, подключенные к электросети с двунаправленной передачей данных в режиме реального времени. Если злоумышленники получают информацию о потребителях, они могут злоупотреблять этой информацией, отслеживать их образ жизни, узнавать, какие приборы они используют, и находятся ли они дома или нет [3].

Данные никогда не должны подвергаться подделке кем-либо или чем-либо в системе. Меры по обеспечению целостности защищают информацию от несанкционированного изменения. Эти меры обеспечивают уверенность в точности и полноте данных. Потребность в защите информации включает как данные, которые хранятся в системах, так и данные, которые передаются между системами, например электронная почта. Для поддержания целостности необходимо не только контролировать доступ на системном уровне, но и дополнительно гарантировать, что пользователи системы могут изменять только ту информацию, которую они законно уполномочены изменять. Таким образом, данные не должны изменяться несанкционированным или необнаруженным образом. Целостность определяется как предотвращение несанкционированного изменения и уничтожения данных, а также означает сохранение и обеспечение достоверности данных. Целостность помогает обеспечить безопасную систему мониторинга в режиме реального времени для интеллектуальной сети.

Ожидается, что энергосистема будет доступна все время. Также важно обеспечить своевременный и надежный доступ и использование информационной системы. Доступность – это защита информационной системы от выхода из строя. Меры доступности обеспечивают своевременный и бесперебойный доступ к системе. Некоторые из наиболее серьезных угроз доступности не являются вредоносными по своей природе

и включают сбои оборудования, незапланированные простои программного обеспечения или проблемы с пропускной способностью сети. Вредоносные атаки включают в себя различные формы саботажа, направленные на причинение вреда организации путем отказа пользователям в доступе к информационной системе. Атаки доступности могут повредить, заблокировать или задержать информацию [4]. Таким образом, доступность означает, что информация должна быть доступна авторизованным сторонам в интеллектуальной сети, когда это необходимо, без ущерба для безопасности. Доступность данных обычно предполагает предотвращение DoS-атак, которые приводят к отключению электроэнергии [5]. Злоумышленники используют информацию, чтобы извлечь выгоду или причинить вред другим. Атаки на конфиденциальность направлены на то, чтобы позволить доступ к информации неавторизованным сторонам [6]. Атаки на целостность направлены на манипулирование исходными данными или вставку ложных данных. Атаки доступности направлены на прерывание подачи питания, задержку или разрыв связи.

2. Атаки на конфиденциальность и меры по их предотвращению

Конфиденциальность позволяет предотвратить несанкционированный доступ к информации. Цель атак на конфиденциальность – попытка украсть информацию, которая должна быть передана или храниться в тайне только между защищенными сторонами. Незаконное считывание памяти устройств, подмена полезной нагрузки, повторные атаки и изменение программы управления – вот некоторые примеры таких атак на интеллектуальную сеть. Сетевое кодирование используется для сохранения конфиденциальности данных. Это обеспечивает конфиденциальность в интеллектуальной сети. Конфиденциальность данных включает в себя и скрытность.

По сравнению с атаками на целостность, атаки на конфиденциальность не стремятся изменить передаваемую информацию. Злоумышленники могут прослушивать каналы связи в интеллектуальной сети, чтобы получить желаемую информацию, такую как потребляемая мощность или номер счета. Типичные примеры – анализ трафика и атаки на прослушивание телефонных разговоров [7]. Можно считать, что атака на конфиденциальность оказывает незначительное влияние на функциональные возможности канала связи в приложениях интеллектуальных сетей.

Атаки с маскировкой также называются подделкой личности. Атаки с использованием спуфинга (англ. spoofing – подмена), такие как подмена MAC-адреса, подмена ARP, подмена IP-адреса, являются незаконной модификацией параметров и являются атаками маскировки. Атаки с подменой идентификационных данных, такие как воспроизведение сообщений, MITM и сетевая подмена, позволяют имитировать

авторизованный ресурс без использования пароля пользователя [8]. Процессы аутентификации необходимы каждому интеллектуальному сетевому устройству, чтобы избежать этих атак.

Без шифрования злоумышленники могут наблюдать и собирать важную информацию. Шифрование защищает информацию от кибератак, делает сеть виртуальной и частной. Атака с перехватом пакетов может быть уменьшена путем использования шлюза безопасности, который передает IP-пакеты благодаря туннелю VPN, который разработан путем встраивания зашифрованного IP-туннеля в общую полезную нагрузку IP-сети. Связь между туннелями VPN защищена с использованием протокола TLS, а также отношения между отдельными сторонами в интеллектуальной сети достигаются с помощью сертификатов X.509, которые аутентифицируют пользователей и обмениваются симметричными ключами.

3. Атаки на целостность и меры по их предотвращению

Целостность означает блокирование несанкционированного изменения или кражи информации. Задержка, воспроизведение и внедрение сообщений нарушают целостность сети. Атаки целостности нацелены на изменение содержания исходных данных, таких как данные учетной записи клиента, значения напряжения датчиков, команды управления, рабочее состояние устройств. Алгоритмы и методы криптографии используются для предотвращения атак на целостность данных. Предлагаются некоторые подходы для защиты от кибератак на целостность, такие как метод снятия отпечатков пальцев и подход на основе надежного сетевого соединения [9]. Нарушение целостности может привести к проблемам безопасности.

Некоторые методы MITM – это измененный источник и назначение пакетов, отравление таблицы маршрутов и скомпрометированные сертификаты. Сетевой трафик должен быть зашифрован с использованием шлюзов безопасности для противодействия атакам MITM. Шлюзы безопасности создают туннели VPN для соединения сетей. Кроме того, они шифруют и дешифруют данные. Другими словами, аутентификация как исходного, так и целевого узлов и шифрование сетевого трафика с помощью шлюзов безопасности являются важными решениями. Кроме того, протоколы TLS обладают внутренними асимметричными криптографическими характеристиками, которые могут немедленно обнаруживать и устранять сбои, чтобы избежать атак MITM.

Атака временной синхронизации (TSA) нацелена на временные данные в приложениях интеллектуальной сети. Важные процессы, такие как оценка местоположения событий и обнаружение неисправностей, во многом зависят от точных данных о времени в интеллектуальной сети.

Схемы аутентификации и сквозное шифрование необходимы для устранения вышеупомянутых атак на целостность в сетях

интеллектуальных энергосистем. Кроме того, злоумышленники должны иметь аутентифицированный доступ к коммуникационным сетям и конфиденциальной информации, чтобы инициировать атаку конфиденциальности или целостности. Следовательно, контроль доступа и аутентификация имеют решающее значение для предотвращения атак на целостность интеллектуальной сети.

4. Атаки доступности и меры по их предотвращению

Атаки доступности предотвращают и могут дестабилизировать авторизованный доступ в интеллектуальной сети. Атаки доступности также известны как DoS-атаки. DoS-атаки направлены на блокировку, повреждение и задержку передачи данных. Это вызывает недоступность сетевых источников. Атаки доступности направлены на перегрузку сетей с использованием различных методов, так что система не может работать должным образом.

Злоумышленники отправляют большие объемы трафика для «затопления» линий передачи данных в сети. Это приводит к потере и невозможности обработки допустимых пакетов данных в сетевом трафике. Доступность является наиболее важным требованием безопасности в интеллектуальной сети, следовательно, против атак доступности должны быть приняты передовые и эффективные меры противодействия. Эффективными решениями являются: фильтрация трафика, подходы к обнаружению аномалий и использование сети с «воздушными зазорами».

Скоординированная атака – самый сложный тип атаки. Поскольку скоординированные атаки могут превосходить обычную защиту, они требуют многоуровневого решения безопасности с надежными подходами. Кроме того, скоординированные атаки нацелены на все аспекты безопасности, требования и компоненты интеллектуальной сети. Таким образом, подходы к безопасности, достигаемые путем анализа требований к кибербезопасности в соответствии с сетевыми уровнями, обеспечат эффективные решения безопасности для приложений умных сетей.

В статье на основе анализа зарубежного опыта рассмотрены и проанализированы угрозы и потенциальные решения для обеспечения безопасного функционирования интеллектуальной сети Интернета вещей.

Кибербезопасность является критически важным аспектом приложений и устройств, входящих в интеллектуальную сеть на основе Интернета вещей.

Предложены подходы к обеспечению кибербезопасности интеллектуальной сети и рассмотрены типы кибератак.

В статье показаны риски безопасности, присущих ИТ-среде, и можно сделать вывод, что почти все аспекты, связанные с ИТ-технологиями в приложениях интеллектуальных сетей, имеют потенциальные уязвимости.

Таким образом, вопросы безопасности в приложениях умных сетей должны подлежать более глубокому изучению, в том числе в целях обеспечения деятельности правоохранительных органов.

Литература

1. Александров А. А., Леонтьева Н. В. Проблемы обеспечения безопасности «Умных городов».
2. D.B. Rawat, C. Bajracharya, Cyber security for smart grid systems: Status, chal– lenges and perspectives, in: SoutheastCon 2015, 2015, pp. 1–6.
3. D.B. Rawat, C. Bajracharya, Cyber security for smart grid systems: Status, chal– lenges and perspectives, in: SoutheastCon 2015, 2015, pp. 1–6.
4. P. Eder–Neuhauser, T. Zseby, J. Fabini, G. Vormayr, Cyber attack models for smart grid environments, Sustain. Energy Grid. Netw. 12 (Supplement C) (2017) 10–29.
5. R.E. Pérez–Guzmán, Y. Salgueiro–Sicilia, M. Rivera, Communication systems and security issues in smart microgrids, in: 2017 IEEE Southern Power Electronics Conference (SPEC), 2017, pp. 1–6.
6. R.K. Pandey, M. Misra, Cyber security threats–Smart grid infra-structure, in: 2016 National Power Systems Conference (NPSC), 2016, pp. 1–6.
7. W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges, Com– put. Netw. 57 (5) (2013) 1344–1371.
8. X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu, Securing smart grid: cyber attacks, countermeasures, and challenges, IEEE Commun. Mag. 50 (8) (2012) 38–45.
9. Y. Yang, T. Littler, S. Sezer, K. McLaughlin, H.F. Wang, Impact of cyber–security issues on Smart Grid, in: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, 2011, pp. 1–7.

Ледовская Маргарита Александровна,
led_ma@mail.ru
Краснодарский университет МВД России

Владимиркина Галина Юрьевна,
Vladimirkina.galina@yandex.ru
Краснодарский университет МВД России

ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ ТЕРРОРИСТИЧЕСКИМИ И ЭКСТРЕМИСТСКИМИ ОРГАНИЗАЦИЯМИ

Аннотация. Рассматриваются основные способы пропаганды террористическими и экстремистскими организациями, занимающие свою позицию исключительно в сети Интернет.

Ключевые слова: Интернет, вербовка, террористические и экстремистские организации, пропаганда, террорист, экстремизм, терроризм.

На сегодняшний день Интернет является самым эффективным способом массового воздействия террористов на общество. Причинами такой популярности сети Интернет среди преступников – является легкость в использовании, анонимность действий, высокая скорость передачи информации, большой охват, незначительные затраты, возможность представлять информацию в виде мультимедийного контента.

Террористические и экстремистские организации используют Интернет для вербовки новых членов, включая террористов–смертников из числа как исламистов, так и экстремистски настроенной молодежи с целью привлечения их сначала в радикальный ислам, а затем и в противоправную деятельность. Кроме того, Интернет используется для формирования лояльно настроенной среды, играющей активную роль в поддержке террористических организаций.

Для противодействия распространения пропаганды идеологии экстремизма и терроризма следует понимать специфику изучаемого вопроса. Для этого следует разобраться в основных направлениях деятельности экстремистских и террористских организаций. Как правило, выделяют исламистскую, праворадикальную и леворадикальную направленность идеологий.

Пропагандистская деятельность исламистской группировки «Исламское государство» нацелена на привлечение в свои ряды как можно большего числа сторонников и на разжигание террористической войны в различных частях мира с целью отвлечения сил мирового сообщества от подавления главных очагов экстремистской угрозы.

Праворадикальные организации, группы нс-скинхедов и автономных праворадикалов большое внимание уделяют пропаганде своих взглядов с помощью социальных сетей и сети Интернет. Главной чертой современной праворадикальной пропаганды является ее соединение:

– с решением какой-либо социальной проблемы (например, с борьбой за сохранение окружающей среды или с противодействием сексуальному насилию над детьми и подростками);

– с общением в группах по интересам (например, по вопросам организации здорового образа жизни или обмену записями определенного музыкального направления).

Современный леворадикализм уделяет значительное место распространению своих идей в широких слоях населения. Особое внимание при этом уделяется пропаганде в сети Интернет, при этом можно выделить следующие основные виды сайтов, в той или иной форме осуществляющих пропаганду леворадикальных идей. Основными видами леворадикальных сайтов следует признать:

– сайты партий;
– межпартийные информационные ресурсы;
– электронные журналы и газеты;
– электронные библиотеки;
– интернет-форумы;
– группы в контакте;
– личные сайты.

Поиск информации данной тематики является базой для удачного противодействия в последующем, так как идентификация таких организаций в сети Интернет может предотвратить негативное воздействие на общество и пресечь их противоправную деятельность. Именно поэтому изучение данного вопроса является актуальным на сегодняшний день, так как большая часть деятельности экстремистов и террористов перешла на информационные площадки сети Интернет, используя открытые источники для распространения своей пропагандистской информации.

Одним из основных применений Интернета террористами является распространение пропаганды. В основном это осуществляется посредством мультимедийных каналов коммуникации – они распространяют свою идеологию, подстрекают к совершению террористических актов, дают практические рекомендации и др.

Интернет может быть использован не только для публикации экстремистских материалов, но также и для налаживания контакта и развития отношений с аудиторией, которая наиболее подвержена влиянию террористической пропаганды. Для вербовки террористические группировки все чаще используют защищенные паролем сайты и порталы

с ограниченным доступом. Доступность и охват Интернета предоставляют террористам доступ к огромному количеству потенциальных новобранцев.

Можно выделить следующие методы, которые используются террористами для вербовки в Интернете.

1. Создание веб-сайтов. Согласно статистике прошлых лет, число сайтов террористической направленности начиная с 1998 года выросло с 12 до 7000. Это дает представление о том, что все чаще террористы выбирают интернет-площадки для коммуникации со своими пособниками и новобранцами, которым обеспечивают онлайн-обучение по подготовке террористических актов.

2. Использование социальных сетей. Террористы распространяют информацию, используя обширные возможности соц-медиа – Twitter, Facebook, YouTube, Vkontakte и другие. Как говорится в сообщении ООН «The use of the Internet for terrorist purposes», такие материалы индексируются поисковые системами, что делает их легкодоступными для потенциальных новобранцев. Только в 2016 году Twitter заблокировал 235 000 аккаунтов экстремистской направленности.

3. Таргетинг. Умения и знания в области психологии, помогают террористам воздействовать на людей, используя психологические уловки. Как правило, таргетинг позволяет выявить целевую аудиторию, наиболее уязвимую к воздействию. Ориентируясь на наиболее уязвимых, восприимчивых и маргинальных членов общества, террористы в своих целях играют чувствами одиночества, слабости, стыда или потребностью в принадлежности к какой-либо социальной группе.

4. Завлечение с помощью медиаконтента: мультфильмы, скетчи. Как правило, самой уязвимой частью населения являются дети, поскольку они не имеют устойчивого психологического восприятия к окружающему обществу. Тем самым, интерес детей террористы добиваются с помощью мультфильмов, фильмов или скетчей, коротких роликов, которые могут являться пропагандой терроризма и экстремизма, оправдывающие насилие и убийство.

5. Использование стриминговых видео-сервисов. Стриминговые видео-сервисы являются платформой для выхода в прямой эфир и трансляции своих действий. Именно одним из таких сервисов в 2016 в Париже воспользовался террорист для трансляции массовых убийств, совершаемых на улице. Видео длительностью 13 минут, на котором были представлены террористические действия в отношении невинных людей после ликвидации террориста еще на протяжении некоторого времени вирусилось в сети Интернет, что позволяло распространять его другим пособникам и представлять это как пример видео-пособие. Так же в самом видео террорист призывал следовать его примеру и устраивать подобные терракты.

6. Создание онлайн видеоигр. Помимо медиаконтента, еще одним действенным способом завлечения молодежной среды в террористические организации является выпуск видеоигр, способные симулировать действия террористов. Играя подросток смог бы представить себя террористом, разработать план нападения или собрать бомбу.

Исследование данного вопроса показало, что сеть Интернет служит одной из главных площадок для размещения своего контента экстремистами и террористами. Однако для результативного и качественного поиска данной информации необходимы знания в области изучаемой нами тематики. На данный момент пробел знаний у сотрудников правоохранительных органов в области экстремисткой и террористической направленности затрудняет своевременное предупреждение и пресечение их противоправной деятельности в сети Интернет.

Литература

1. Демянчук Е.В. Оперативно-розыскные мероприятия и методы по выявлению и пресечению пропаганды идей терроризма и экстремизма в сети Интернет. М., 2007.

2. Зыгаръ М. Пропаганда террора // КоммерсантЪ. Первый рейтинг. 2004. Январь.

Ледовская Маргарита Александровна,
led_ma@mail.ru
Краснодарский университет МВД России

Шандакова Арина Сергеевна,
arixa2012@yandex.ru
Краснодарский университет МВД России

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВАНИЯ ПРОТИВОДЕЙСТВИЯМ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИСТСКОЙ СИМВОЛИКИ

Аннотация. Обозначены актуальные проблемы нормативно–правовой базы противодействия распространению экстремистской символики. Предложены пути решения проблемы.

Ключевые слова: экстремизм, символика, интернет, нормативно–правовые источники.

С каждым днем связь между современным обществом и информационными технологиями становится только сильнее. В данный момент практически каждому знакомо понятие мировой сети Интернет,

что говорит о ее влиянии не только на отдельных индивидов, а на социум в целом. Трудно представить нашу жизнь без телефона, компьютера или телевизора. Бесспорно, эти устройства приносят пользу человеку позволяя совершать обмен информацией на огромные расстояния, и распространять ее на большие социальные группы. В этом и заключается опасность влияния информационно-коммуникативных технологий на общество. Лидеры экстремистских группировок, в том числе и праворадикального характера, всеми силами стремятся распространить идеологию и лозунги своего формирования, для завлечения граждан и организаций в праворадикальную среду, тем самым укрепляя свои позиции среди населения государства.

Одним из критериев экстремистской идеологии является ее символика.

Символика – это совокупность знаков, изображений, эмблем, символов и иероглифов, используемых группой лиц, организацией, общественным или политическим образованием, государством для своего обозначения и выражения, среди идентичных формирований.

Экстремистская символика представляет собой комплекс обозначений той или иной группы или организации, выражающий ее принципы, функции и основные направления деятельности. Также она используется для коммуникации членов группировки между собой и взаимодействия с другими объединениями. Важной отличительной чертой будет вступившее в законную силу судебное решение о признании организации, в учредительных документах которой указывается эта символика, организацией экстремистской направленности, что подразумевает запрет ее деятельности, и, соответственно, ограничение распространения ее символики.

С 06.01.2013 года в федеральном законе № 114 «О противодействии экстремистской деятельности» предусмотрено официальное понятие экстремистской символики. Оно претерпело множество корректировок и в настоящий момент звучит так:

Символика экстремистской организации – символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

В настоящее время в административное и уголовное законодательство Российской Федерации вносятся изменения, связанные с действиями экстремистской направленности. Например, впредь пресекаются и преследуются по закону деяния направленные на «…публичное оскорбление памяти защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны» (ст. 354.1

УК РФ Реабилитация нацизма). Административным кодексом также предусмотрена ответственность за «…публичное оскорбление памяти защитников Отечества и ветеранов Великой Отечественной войны» (ст. 3.5 и 13.15 КоАП РФ).

Под публичным оскорблением ветеранов Великой Отечественной войны понимается оправдание действий нацистской Германии, а именно методов захвата власти, истребления и угнетения по расовому и национальному признаку, тех групп и этносов, которые отличаются по цвету кожи, вероисповеданию, идеологии и т. д. Лидеры и участники праворадикальных организаций экстремистской направленности распространяют нацистскую символику и цвета, тем самым признавая гонения по национальной и расовой принадлежности в обществе как норму. В этом заключается опасность воздействия экстремистской символики в первую очередь на подрастающее поколение и молодежные субкультуры, на которые легко оказывают влияние праворадикальные объединения и движения, путем завлечения подростков в свои группировки и дальнейшей их вербовки.

В настоящее время процесс социализации молодежи тесно связан с глобальной сетью Интернет. В связи с чем государству как образованию, созданному для защиты жизни и здоровья своих граждан, необходимо применять меры направленные на предотвращение распространения экстремистских материалов среди населения, особенно подростков и молодежных объединений.

Прежде всего, необходимо понимать, что каждая праворадикальная организация следует своей идеологии вследствие чего у нее имеется определенная символика, которая выполняет следующие функции:

– представляющая функция, выражает основную идею создания и принципы, характеризующие организацию, а также возможные цели, которые она преследует;

– апологетическая функция, направлена на оправдание осуществляемой противоправной деятельности;

– воспроизводящая функция, помогает вербовать в группировку или организацию новых сторонников, преимущественно подростков;

– генетическая функция, говорит об истории создания и развития организации, а также о зарождении ее идеологии и основных принципах;

– объединяющая функция, помогает скооперироваться членам группировки или организации для определения основных направлений деятельности организации и решения возникающих проблем;

– идентифицирующая функция, указывает на отличительные черты идеологии группировки от идентичных образований и выражается с помощью различной интерпретации изображений, иероглифов и символов;

В своей статье Чернега И.В. говорит об одной специфической черте обнаружения преступлений экстремистского характера в Интернете: «при

выявлении правоохранительными органами размещения информационных материалов с признаками экстремизма в сети Интернет сложно определить на практике непосредственно тех лиц, кто осуществляет распространение данной информации, получить необходимые данные о них» [7]. Проблема заключается в том, что в глобальной сети очень легко распространять информацию анонимно, без указания своих личных данных и месте проживания. Этот факт значительно усложняет работу сотрудников правоохранительных органов по противодействию экстремизму, вынуждая их разрабатывать новые методы выявления лиц, публикующих экстремистскую символику в Интернете, тем самым распространяя ее среди пользователей. О них будет изложено в следующей главе.

Еще одна специфическая черта праворадикальной символики ее разнообразие. Каждый день лидеры праворадикальных организаций создают новые иероглифы, знаки и изображения, на смену признанным экстремистской символикой. И так как Интернет представляет собой глобальную сеть (около 100 млн граждан Российской Федерации используют информационно-телекоммуникационную сеть «Интернет»), содержащую огромнейшие массивы информации, процесс выявления и ограничения запрещенных материалов становится довольно затруднительным. Несмотря на сложность, правоохранительные органы РФ справляются с задачей, так как находятся на постоянном контакте на этом направлении. Сотрудники ЦПЭ обладают определенными знаниями идеологий праворадикальной направленности, что позволяет им проводит анализ символики праворадикального характера и определять ей компоненты:

- нацистские и неонацистские символы;
- традиционные цвета нацисткой Германии и Третьего Рейха;
- символику коллаборационнистких отрядов и формирований;
- элементов, доказывающих преемственность между нацистской символикой и символиками российских праворадикальных объединений, признанных экстремистскими;
- выражение оправдания насилия по расовому и национальному признаку в праворадикальной символике и атрибутике.

Специфика выявления экстремистской символики и выявления праворадикальных организаций по этой символике имеет конкретные различия. Например, эффективнее не сразу предъявлять обвинения лицу, распространяющему запрещенные изображения, а проследить за ним и выявить по нанесенному изображению праворадикальную группировку, к которой он принадлежит, а также установить характерные черты ее идеологии. Произведя анализ экстремистского символа можно сделать выводы о степени социальной опасности группы и определить факт действия уже известного праворадикального сообщества, трансформации старого или возникновения нового праворадикального сообщества.

Как уже говорилось ранее, определить личность человека, публикующего символы экстремистского характера в глобальной сети Интернет непростая задача. Однако если это все-таки удается, ставится вопрос о привлечении его к административной ответственности. Однако если выяснится то, что публикацию экстремистской символики лицо совершало с расчетом разжечь ненависть, либо вражду, а также унизить достоинства человека, либо группы лиц по расовому или национальному признаку, а равно языку, происхождению или религиозным убеждениям, ставится вопрос об уголовном преследовании.

Главная специфичная особенность распространения экстремистской символики в Интернете заключается в том, что наиболее негативное влияние она оказывает на умы подростков, стремящихся к самовыражению за счет участия в праворадикальных организациях и изучения запрещенной символики. Тем самым молодежь как бы относит себя к группе «избранных» личностей, способных, по их мнению, диктовать свои условия существования государства. В большинстве это превознесение определенной расы (национальности), ксенофобия и угнетение других народов, этносов, групп, ради «сохранения чистоты крови».

В заключении отметим, что на сегодняшний день такое масштабное и многонациональное государство как Российская федерация обладает хорошо проработанным и эффективным в применении нормативно–правовым полем противодействия распространению экстремистской символики и иных структурных элементов идеологии организаций, направленных на насильственное изменение политического строя в стране самыми жесткими способами. В свою очередь сотрудники правоохранительных органов, а именно центров противодействия экстремизму и терроризму круглосуточно занимаются своевременным выявлением и ограничением сведений, запрещенных законодательством и признанных экстремистскими материалами, опасных в первую очередь для подростков и молодежных объединений, защищая молодое поколение от радикализации и криминализации.

Литература

1. Чернега И.В. Об актуальных вопросах противодействия размещения в сети «Интернет» запрещенной информации//вестник науки и образования. Том 2. – 2017. – № 6 (30).

2. Водяная М.Ю., Ляшук А.В. Противодействие проявлениям экстремизма при осуществлении административного надзора и судебного контроля в сфере связи, информационных технологий и массовых коммуникаций // Полицейская деятельность. – 2020. – № 5.

Макуха Максим Юрьевич,
mmkrdu@yandex.ru
Краснодарский университет МВД России

Богданов Дмитрий Сергеевич,
bdkrdu@yandex.ru
Краснодарский университет МВД России

Горюн Кристина Николаевна,
kngoryun@yandex.ru
Краснодарский университет МВД России

К ВОПРОСУ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ЛИЧНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ИСОД МВД РОССИИ

Аннотация. Обозначены актуальные проблемы обеспечения конфиденциальности личности сотрудников легендированных подразделений в ИСОД МВД России. Предложены пути решения проблемы.

Ключевые слова: ИСОД, ВИСП, СВКС-М, Адресно-телефонный справочник.

Сегодня невозможно представить деятельность МВД России без использования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России, что объясняется большим количеством задач оперативно-служебной и повседневной деятельности, решаемых с их использованием.

К прикладным сервисам повседневной деятельности относятся такие сервисы как:

- сервис электронного документооборота (СЭД);
- сервис электронной почты (СЭП);
- ведомственный информационно–справочный портал (ВИСП);
- сервис видеоконференцсвязи МВД России (СВКС-М).

С каждым из вышеперечисленных сервисов большинство сотрудников МВД России сталкивается практически каждый день. Далее мы рассмотрим работу сервисов ВИСП и СВКС-М, так как существует проблема обеспечения конфиденциальности личности сотрудников органов внутренних дел, работающих в легендированных подразделениях.

Ведомственный информационно-справочный портал.

Областью применения ВИСП являются такие виды повседневной деятельности подразделений МВД России как:

- получение справочной информации;

– получение информации об организационно-штатной структуре МВД России;

– работа с адресно-телефонным справочником;

– освещение новостей и информирование о событиях МВД России.

Основными целями использования ВИСП сотрудниками и должностными лицами подразделений МВД России центрального аппарата и территориальных органов МВД России являются:

– получение информации, касающейся повседневной деятельности МВД России, а также информации, касающейся использования сервисов ИСОД МВД России;

– использование общих информационных ресурсов для выполнения своих служебных обязанностей;

– ознакомление с организационно-штатной структурой и информацией о сотрудниках МВД России;

– снижение временных затрат на сбор, обработку и поиск информации [1].

Интерфейс ВИСП содержит ссылки на следующие разделы:

– «Адресно-телефонный справочник»;

– «Новости, события и НТИ»;

– «Вопросы и ответы»;

– «Сервисы ИСОД»;

– «Поиск по ВИСП».

Раздел «Адресно-телефонный справочник» предназначен для поиска и просмотра организационно-штатной структуры, карточки сотрудника ведомства и карточки организации МВД России.

Для обращения к разделу необходимо выбрать пункт «Адресно-телефонный справочник» области «Верхнего меню», после чего откроется форма, представленная на рис. 1.

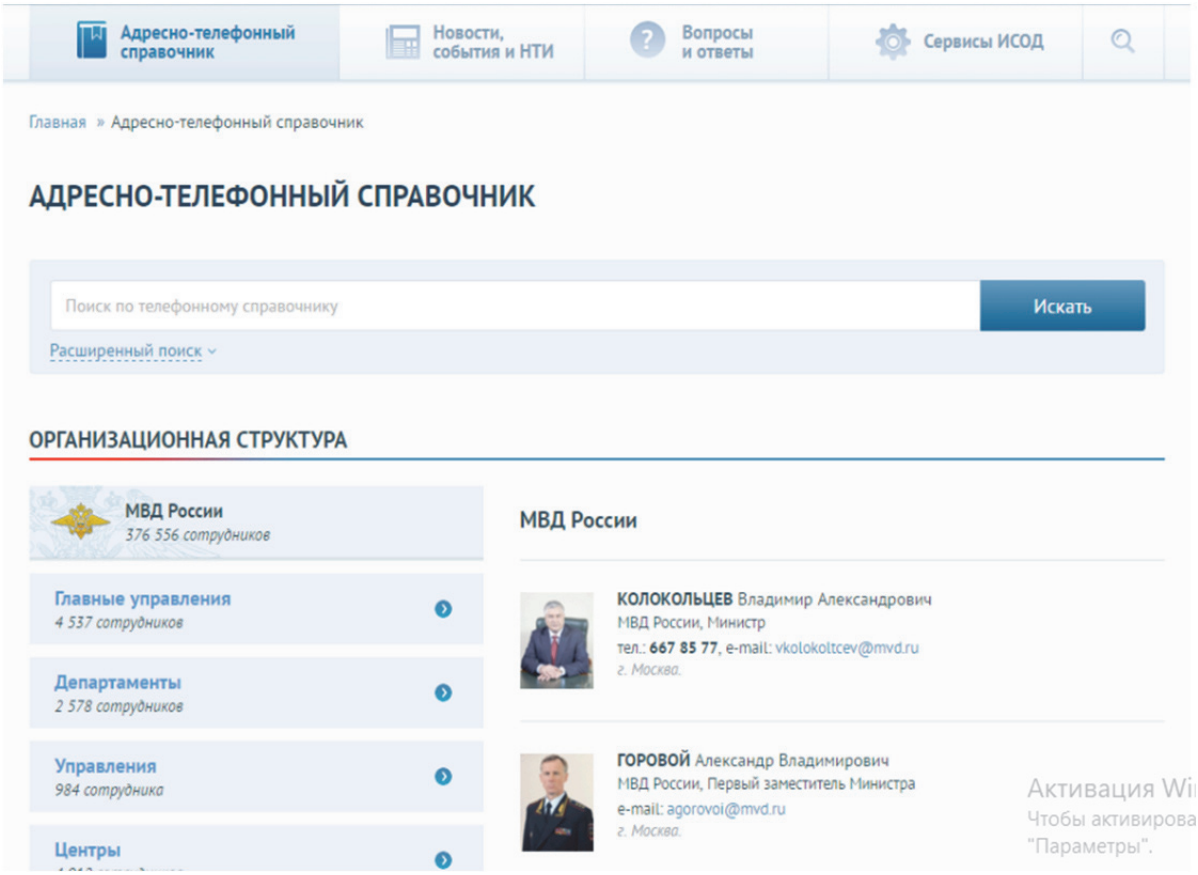


Рис. 1. Вид раздела «Адресно–телефонный справочник»

Для выполнения поиска по сотрудникам выбранной организации или подразделения в области «Поиск по телефонному справочнику» необходимо установить курсор в область поиска и ввести поисковое слово.

При нажатии ссылки «Расширенный поиск» отображаются поля для поиска: «Фамилия», «Имя», «Отчество», «Город», «Должность», «Номер телефона», «Подразделение» и кнопка «Очистить поля». Вид расширенного поиска по сотрудникам представлен на рис. 2.

Результаты расширенного поиска являются более точными, так как поиск осуществляется по полному соответствию поискового значения в каждом указанном поле.

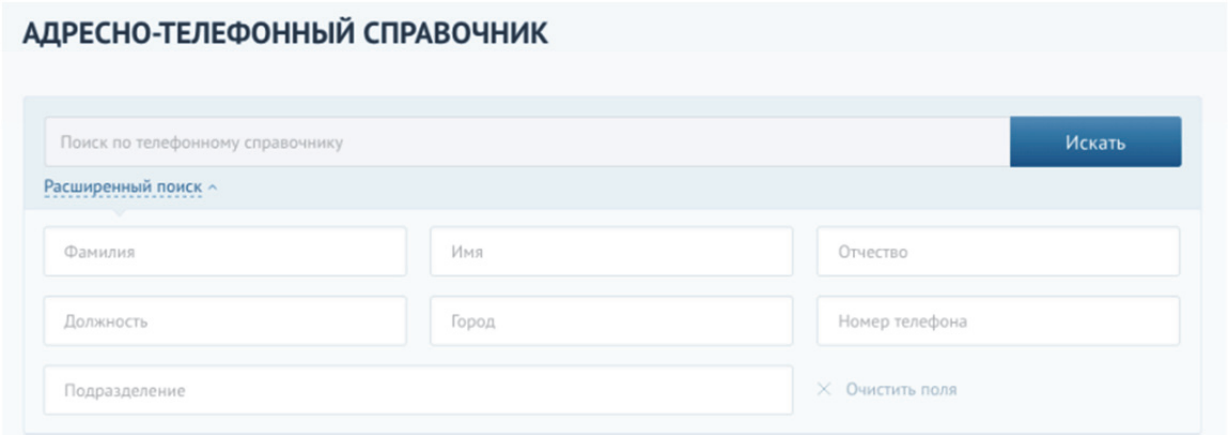


Рис. 2. Вид расширенного поиска по сотрудникам

Сервис видеоконференцсвязи МВД России.

Приложение «Специальная видеосвязь» предназначено для предоставления возможности использовать видеоконференцсвязь, а также дополнительные средства взаимодействия для повседневного общения пользователей системы.

СВКС–М предоставляет возможность проведения групповых, симметричных, ассиметричных и ролевых видеоконференций, а также осуществления видеозвонков [2].

Помимо основных функций клиентское программное обеспечение предоставляет возможность осуществлять поиск пользователя (рис. 3).

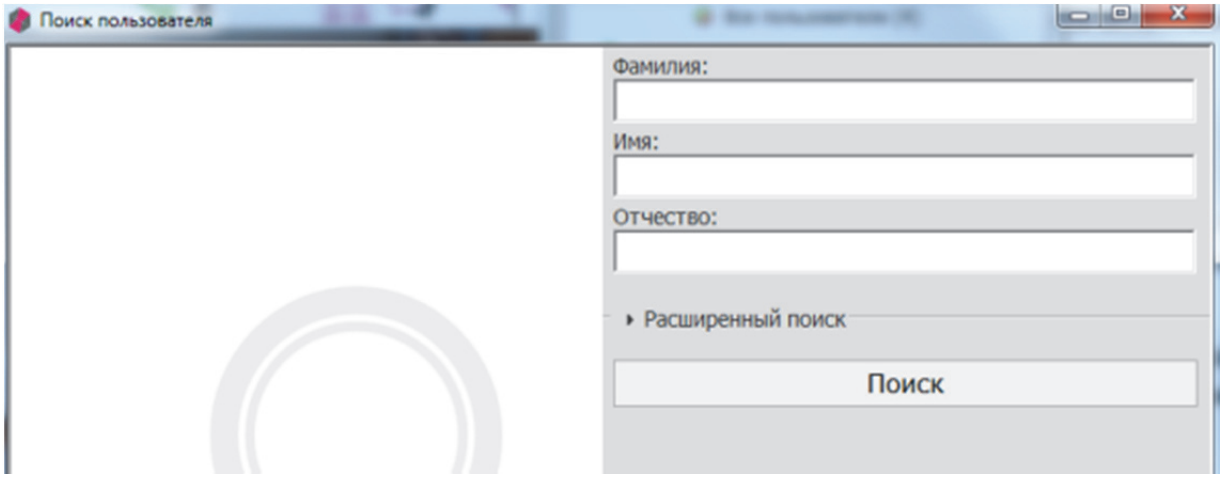


Рис. 3. Окно поиска пользователей

Для снижения результатов предусмотрена возможность осуществления расширенного поиска, который предоставляет возможность поиска по регионам, а также добавляет дополнительные поля критериев поиска «Должность» и «Подразделение» (рис. 4).

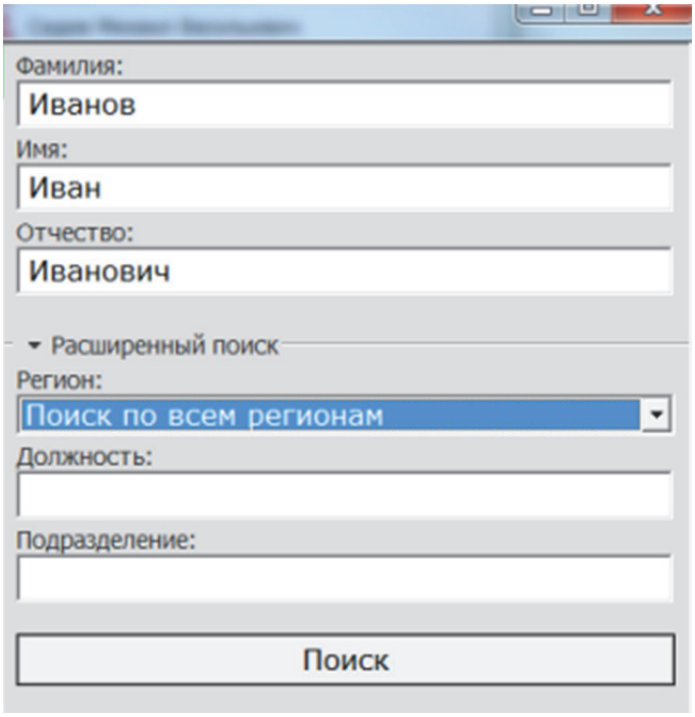


Рис. 4. Расширенный поиск пользователей

Вышеописанные сервисы предоставляют большие возможности по оперативному взаимодействию пользователей, однако, расширенный поиск СВКС-М в нарушение конфиденциальности личности позволяет определить принадлежность сотрудников к легендированным подразделениям.

На рисунках 5 и 6 представлен результат расширенного поиска, где в графе «Подразделение» указано в первом случае «БСТМ ГУ МВД России по Краснодарскому краю», а во втором «ОПБ ГУ МВД Росси по Краснодарскому краю». Результатом поиска является 57 и 64 совпадения соответственно. Аналогичные результаты можно наблюдать и в других регионах. В целях обеспечения конфиденциальности личности сотрудников данных подразделений на рисунках частично уничтожена часть информации, касающаяся фамилии, имени и отчества.

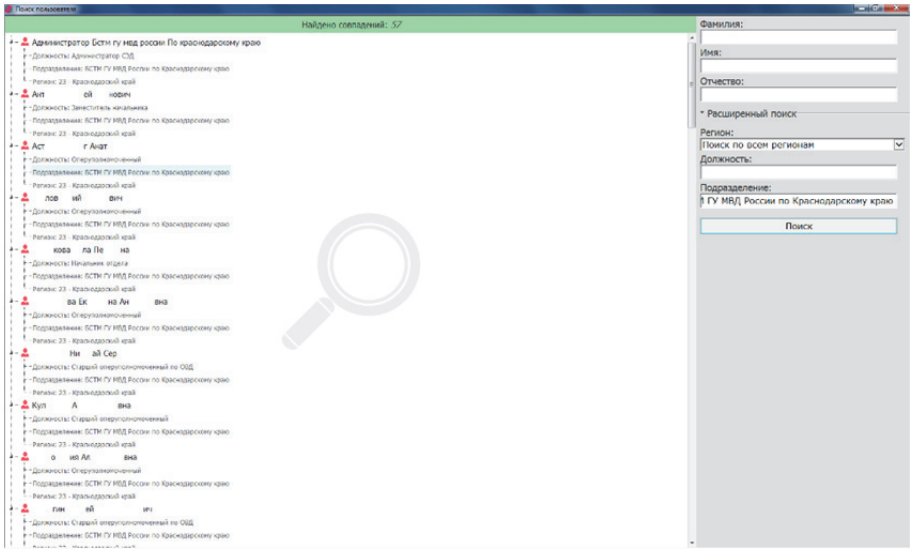


Рис. 5. Расширенный поиск пользователей БСТМ ГУ МВД России по Краснодарскому краю

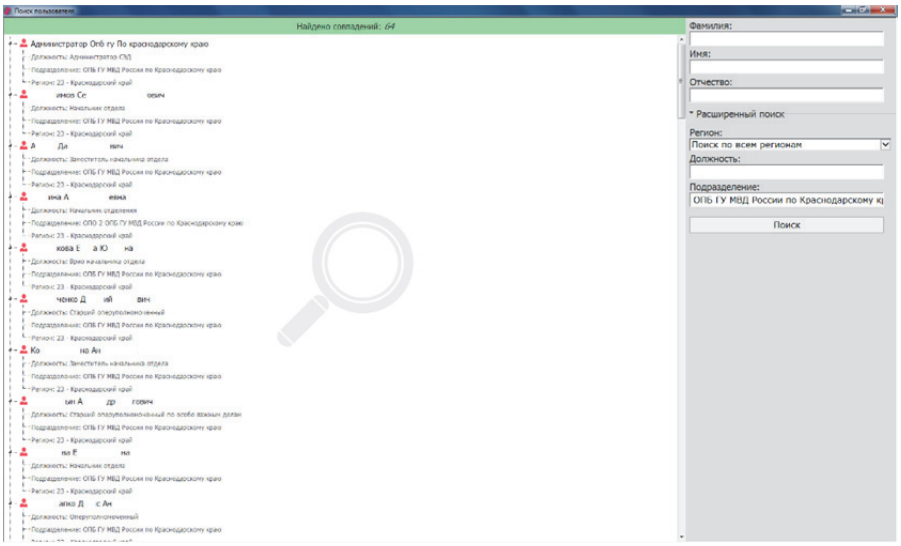


Рис. 6. Расширенный поиск пользователей ОПБ ГУ МВД Росси по Краснодарскому краю

Стоит отметить, что информация о данных сотрудниках отсутствует в адресно-телефонном справочнике ВИСП. Результат расширенного поиска в адресно-телефонном справочнике по сотрудникам БСТМ и ОПБ ГУ МВД России по Краснодарскому краю представлен на рисунках 7 и 8. Отсутствие в ВИСП какой-либо информации о сотрудниках вышеуказанных подразделений говорит о том, что она не подлежит ознакомлению широкому кругу лиц.

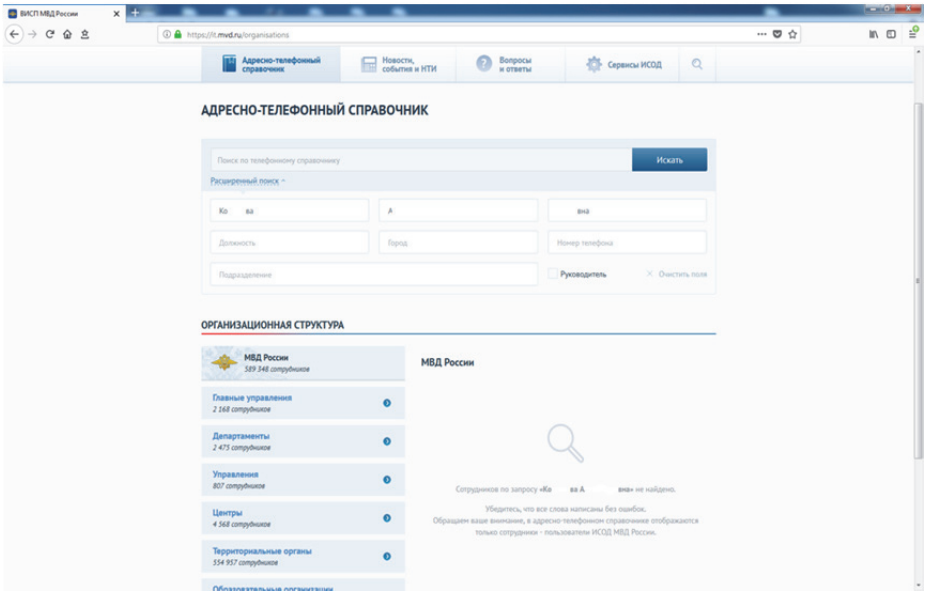


Рис. 7. Расширенный поиск сотрудника БСТМ ГУ МВД России по Краснодарскому краю

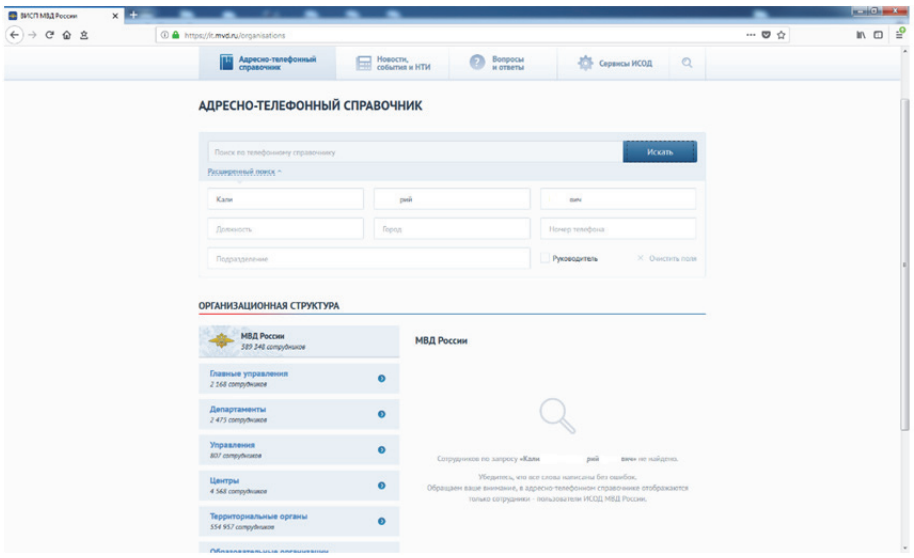


Рис. 8. Расширенный поиск сотрудника ОПБ ГУ МВД России по Краснодарскому краю

Можно сделать вывод о необходимости исключения возможности получения информации о принадлежности сотрудников МВД России к легендированным подразделениям при помощи СВКС-М. В целях устранения указанной проблемы мы предлагаем:

– добавить возможность осуществлять расширенный поиск по подразделениям только из предложенных вариантов, в которых будут отсутствовать легендированные подразделения;

– заменить информацию о занимаемой должности сотрудников, проходящих службу в легендированнных подразделениях на должности иных подразделений.

Указанные предложения позволят устранить проблему нарушения конфиденциальности личности сотрудников легендированных подразделений в ИСОД МВД России с сохранением возможности использования вышеописанных сервисов, в случае необходимости.

Литература

1. Руководство оператора. Прикладной сервис доступа к ведомственному информационно-справочному порталу. Москва 2016, – 83 с.

2. Руководство администратора сервера видеоконференцсвязи СВКС-М. Москва 2015, – 35 с.

Малофей Александр Олегович,
yzorsv@gmail.com
Ставропольский филиал
Краснодарского университета МВД России

Малофей Олег Павлович,
opmalofey@yandex.ru
Институт математики и информационных технологий
имени профессора Н.И. Червякова
Северо-Кавказского федерального университета

ИСПОЛЬЗОВАНИЕ НАБОРА МАЖОРИТАРНЫХ РЕШАЮЩИХ ПРАВИЛ В УСЛОВИЯХ ПОМЕХОВОГО ВОЗДЕЙСТВИЯ

В любой информационно-телекоммуникационной системе составной частью является система передачи информации (СПИ). Зачастую террористическая организация обладает в совокупности достаточно высоким уровнем технической оснащенности, что позволяет им использовать устройства, создающие преднамеренные помехи (УПП) в канале связи СПИ. В условиях воздействия такого рода радиопомех во всем спектре частот создается неравномерный уровень помехового воздействия, при котором ширина спектра, превышает полосу частот сигнала. При этом требуется управление группами антитеррористической борьбы путем использования средств связи. В случае постановки мощной широкополосной помехи во всем разрешенном диапазоне частот известные методы борьбы с ней, такие как изменение мощности излучения передатчика, периода выхода в эфир, смены частотных каналов и другие

окажутся не эффективными. В этом случае в требуемом радиусе связь будет отсутствовать. Следовательно, чтобы осуществлять эффективное управление группой антитеррористической борьбы в таких условиях необходимо обеспечить радиосвязь приемлемого качества в заданном районе. Одним из способов повышения достоверности принимаемой информации будет применение кодовых методов. Если в требуемом радиусе имеется совокупность абонентских станций (АС) у которых обязательно присутствует такой элемент как приемник, то получателю информации потребуется повысить достоверность принимаемых сообщений. Структурная схема такого приемника представлена на рисунке 1. Для доведения сообщения заданной длины *l*, требуется *M* повторений, число которых конечно. Одной из основных характеристик качества канала в сети, использующей в качестве среды распространения свободное пространство, является вероятность ошибки элементарного символа в сообщении.

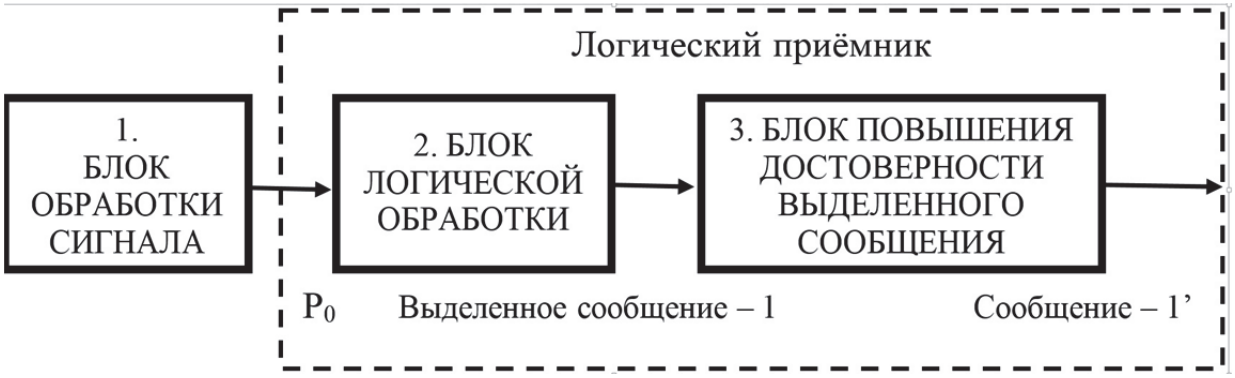


Рис. 1. Структурная схема приемника АС

При таких условиях передача информации в канале связи чаще всего осуществляется в метровом диапазоне волн. В представленной структурной схеме приемника АС повышение достоверности информации, принимаемой из канала, использующего в качестве среды распространения свободное пространство, осуществляется в блоке логической обработки (БЛО) (рис. 1, блок 2). Так как УПП создают высокий неравномерный уровень помех во всем диапазоне рабочих частот штатных радиосредств метрового диапазона, то известные методы повышения достоверности не обеспечат передачу сигнала для управления группой антитеррористической борьбы на требуемое расстояние. Наиболее оптимальным будет применение кодовых методов повышения достоверности принимаемой информации, одним из которых является метод мажоритарного декодирования, причем в работу включаются решающие мажоритарные проверки (РМП) принятого сообщения на всем множестве полученных повторов. Отличительной особенностью здесь будет сравнение одноименных символов каждого повторения. При этом на

каждом повторе сообщения учитываются только РМП очередного шага. РМП предыдущего шага запоминаются и не учитываются при поразрядной обработке сообщения.

Таким образом, при получении трех повторов М=3 возможно использование РМП два из трех (2х3) (происходит одна проверка), при М=5 будут использоваться РМП 2х3 (происходит три проверки, так как не учитывается та проверка 2х3, которая проведена при М=3), при М=5 – 1 РМП 2х3 (6 проверок) и РМП 3х5 (1 проверка) и т. д. [2]. На рис. 2 представлена схема процесса применения проверок одноименных символов в принимаемом сообщении при мажоритарном декодировании пяти повторов.

Симв *l* / № повт	1	2	3	…	*n*
1	❶			…	
2	❷	❷		…	
3	❸	❸	❸	…	
4		❹	❹	…	
5			❺	…	

Рис. 2. Процесса применения проверок

Число необходимых РМП для заданного числа сравнений (либо 2х3, либо 3х5 и т. д.) при получении M повторов вычисляется как число сочетаний из M по N в каждом (1):

$$C_M^N = \frac{M!}{N!(M-N)!} \qquad (1)$$

где M – число полученных повторов, N – число повторов по которым производится сравнение [6].

При накоплении минимального числа повторений, например, пяти потребуется найти сколько решающих мажоритарных правил необходимо, чтобы обеспечить требуемую достоверность принимаемого сообщения. Для этого возьмем все сравнения, которые определяют решающее правило на нужном количестве повторений и вычитаем сравнения, проведенные на предыдущем повторении. Чтобы оценить эффективность применения таких алгоритмов повышения верности сообщений понадобится оперировать понятием эквивалентной вероятности ошибки. Этот

численный показатель меняется в зависимости от применения того или иного набора решающих правил с мажоритарной проверкой.

Применение наборов решающих правил с мажоритарной проверкой обеспечивает повышение достоверности сообщения и, соответственно, снижение вероятности ошибки элементарного символа в принимаемом сообщении [5, 6, 7]. Тогда вероятность правильного приема сообщения по РМП типа 2х3 равна: $\alpha = (1 - P_{э1})'$, а эквивалентная ей вероятность ошибки при этой РМП определяется так $P_{эi} = P_0^3 + C_3^2 \cdot P_0^2 \cdot (1 - P_0)$.

Для РМП 3х5 соответственно имеем $b = (1 - P_{э2})'$, где $P_{э2} = P_0^5 + C_5^4 \cdot P_0^4 \cdot (1 - P_0) + C_5^3 \cdot P_0^3 \cdot (1 - P_0)^2$.

Обобщенная формула для нахождения эквивалентной вероятности ошибки на элементарный символ при выборе произвольного РМП – $P_э^{N\_M}$ имеет вид (2):

$$P_э^{N\_M} = P_0^M + \sum_{i=1}^{N-1} C_M^{M-1} \cdot P_0^{M-1} \cdot (1 - P_0)^i = \sum_{i=1}^{N-1} C_M^{M-1} \cdot P_0^{M-i} \cdot (1 - P_0)^i \quad (2)$$

В некоторых случаях, при длительном снижении качества канала связи, в условиях преднамеренных помех, целесообразно введение дополнительной избыточности путем увеличения числа повторов сообщения с последующей мажоритарной обработкой и исправлением ошибок определенной кратности. Данную процедуру отражает введение в алгоритм мажоритарной обработки дополнительного анализа группы по первому и последним двум повторениям. Это позволит повысить помехоустойчивость приема в условиях сложной сигнально–помеховой обстановки до величины $P_{э5}$ (на рисунке 3). Причем $P_{э5} = P_0^m$ при *m*=3, *N*=5.

Возникает необходимость анализа всех возможных групп повторений при выбранном *N*=5. Это достигается анализом последней группы первых двух и последнего повторений. Теперь, когда получен полный набор мажоритарных правил, вероятность $P_{эi}$ примет вид:

$P_{э6} = (2m - 1)P_0^{n+1}$ при *m*=3, *N*=5

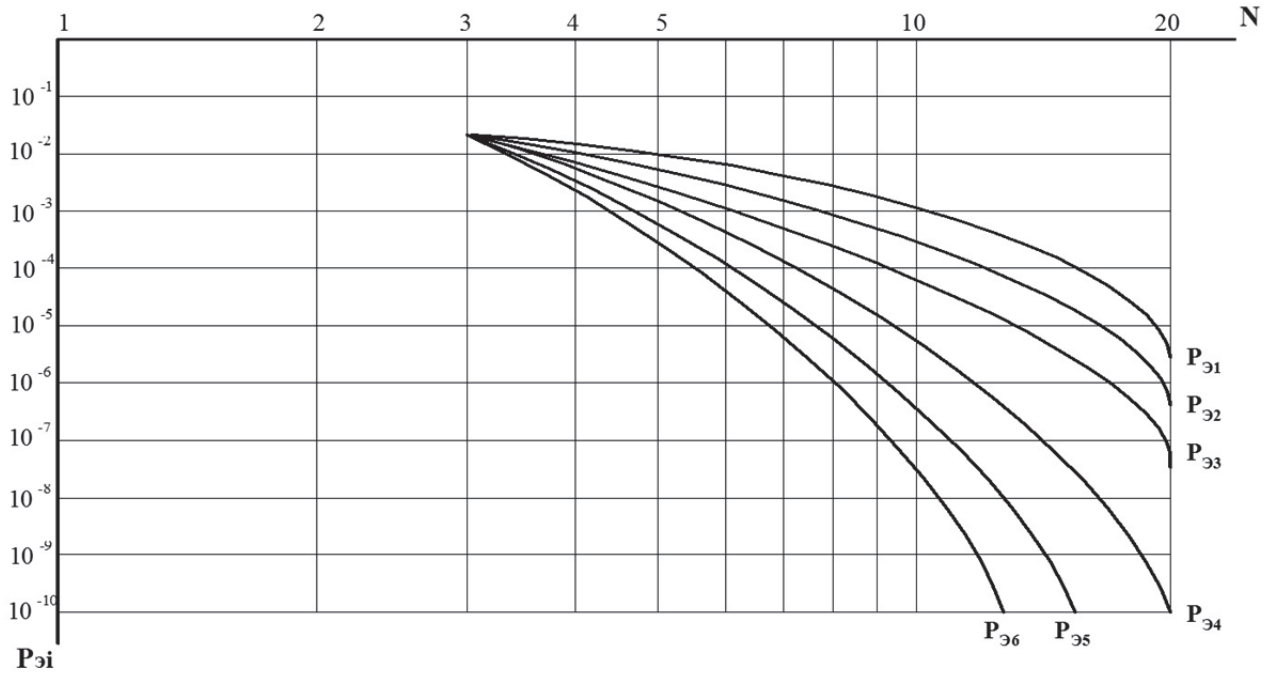


Рис. 3. Зависимость вероятности Рэi от числа повторений N; $P_0 = 10^{-1}$

Итак, при выбранном *N*=5 вероятность искажения единичного символа в кодовой комбинации $P_{э1} = 10P_0^3$ [1].

Зависимость $P_{эi} = f(N, F)$ от количества повторов N и наборов применяемых мажоритарных решающих правил, приведена на рисунке 3. Здесь наглядно видно, что выполняется неравенство $P_{э1} > P_{э2} > P_{э3} > P_{э4} > P_{э5} > P_{э6}$.

Применяемые в устройстве коррекции ошибок расширенные наборы решающих мажоритарных правил можно увидеть, например, в [3, 4], где реализован полный набор таких процедур для пяти повторений.

Необходимую верность доведения сообщения в условиях преднамеренных помех, создаваемых УПП, могут обеспечить путем многократной передачи кодовой комбинации методы повышения достоверности, использующие мажоритарное декодирование, которые позволят осуществить связь с вероятностью 0,9 на рассматриваемых расстояниях.

Литература

1. Малофей А.О. Методы повышения достоверности принимаемой информации при энергетическом подавлении каналов связи, во время проведения спецопераций. В сборнике: Актуальные проблемы безопасности жизнедеятельности и физической культуры в XXI веке: интеграция науки и практики: материалы VII Междунар. заоч. науч.-практ. конф. 2019. С. 127–132.

2. Малофей А.О., Малофей О.П. Некоторые особенности алгоритмов цикловой синхронизации информации, циркулирующей в системах связи силовых структур с каналами низкого качества. В сборнике: Математические методы и информационно–технические средства: материалы XV Всерос. науч.-практ. конф. 2019. С. 117–121.

3. Малофей А.О., Малофей О.П., Малофей Ю.О., Копытов В.В. Устройство коррекции ошибок с расширенным набором решающих правил. Патент на изобретение № 99101022/20(000974) от 18.01.1999 г.

4. Малофей О.П., Малофей А.О., Харечкина Ю.О., Харечкин А.Н. Модифицированное устройство коррекции ошибок. Патент на изобретение RU 2635253 C1, 09.11.2017. Заявка № 2016127940 от 11.07.2016.

5. Малофей О.П., Малофей А.О., Шаньгина А.Е. Сравнительный анализ алгоритмов первичной обработки кодов с повторением. В сборнике: Научно-методические проблемы профессиональной и служебной подготовки в органах внутренних дел России. Электронный сборник материалов всероссийской научно-практической конференции. 2017. С. 205–209.

6. Обнаружение и исправление ошибок в дискретных устройствах / под. ред. В.С. Толстякова. – М., Сов. радио, 1972.

7. Щувалов В.П. Прием сигналов с оценкой их качества. – М: Связь. 1979.

Миненко Дмитрий Алексеевич,
minenko-krd@yandex.ru
Краснодарский университет МВД России

ИСПОЛЬЗОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ ПРИ ПРОВЕДЕНИИ КОНТРТЕРРОРИСТИЧЕСКИХ ОПЕРАЦИЙ

Аннотация. Обозначены тенденции использования БПЛА в целях совершения противоправных действий и террористических актов. Проведен обзор способов и некоторых технических средств противодействия БПЛА.

Ключевые слова: БПЛА, «Пищаль-ПРО», «Персей-201», «Сапсан-Бекас», «СМЕРЧ».

Примерно с 2005 года в мире произошел большей скачек в развитии БПЛА, особенно малогабаритных. К ним относятся микро- и мини-БПЛА ближнего радиуса действия – взлетная масса которых до 5 кг, дальность действия до 25–40 км. Как правило эти дроны могут использоваться для разведки местности с воздуха и получения изображения в режиме реального времени при использовании различной фото и видеоаппаратуры.

Однако у прогресса в этой области есть обратная сторона. Имеющиеся в продаже БПЛА, все больше по своим характеристикам становятся схожи с профессиональными БПЛА. Разработчики постоянно совершенствуют существующие и выпускают новые модели дронов. Кроме того, на рынке имеется широкий выбор конструктивных элементов, позволяющих не только собирать любительские БПЛА с произвольными характеристиками, но и модернизировать по своему усмотрению, имеющиеся в пользовании у частных лиц БПЛА. [1]

Все вышеуказанное предоставляет практически безграничные возможности для совершения противоправных действий на расстоянии, а также без непосредственного участия человека. Так злоумышленник, находясь в километре или более от объекта, оснащенного традиционными системами защиты, получает возможность вести шпионаж с воздуха, наблюдение за частной жизнью. С помощью БПЛА возможно осуществлять заброс за охраняемый периметр запрещенных предметов или вывоз ценностей в обход пунктов контроля и досмотра. Учитывая растущую по всему миру угрозу терроризма, можно ожидать атаки на людей при проведении массовых мероприятий, на объекты жизнеобеспечения и чувствительные элементы инфраструктуры с применением БПЛА, несущих взрывные устройства. Также использование БПЛА дает возможность членам экстремистских организаций вести видеосъемку в районе проведения контртеррористических операций и в режиме реального времени получать информацию о силах и средствах, задействованных в проведении операции. Позволяет контролировать перемещение личного состава, что дает возможность оказания более организованного сопротивления.

Таким образом, в настоящее время остро встает вопрос о способах и методах обнаружения и блокирования БПЛА в целях повышения антитеррористической защищенности административных зданий и сооружений органов государственной власти, объектов жизнеобеспечения, мест массового пребывания граждан. Также существует необходимость в развитии мобильных комплексов обнаружения БПЛА при проведении контртеррористических операций с целью, перехвата, подавления и ликвидации БПЛА противника. [2]

В настоящее время меры противодействия этому новому типу угроз на следующие категории: нормативно–правовое регулирование использование БПЛА, обнаружение БПЛА на расстоянии, подавление и уничтожение БПЛА в полете.

К нормативно-правовому регулированию использования БПЛА относится Федеральный закон от 30 декабря 2015 г. № 462-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации в части использования беспилотных воздушных судов».

Задачу обнаружения БПЛА решают несколькими способами:

– Анализ следа акустического сигнала. Микрофонная решетка принимает акустический сигнал двигателей БПЛА. Далее сигнал анализируется и сравнивается с известной диаграммой направленности сигнала БПЛА. Если параметры сигналов совпадают, происходит обнаружение беспилотного летательного аппарата.

– Оптический анализ воздушного пространства. Осуществляется с использованием видеокамер или массивов камер. Данные изображения обрабатываются в режиме реального времени для распознавания траектории полета;

– Анализ тепловой сигнатуры. Для контроля окружающей среды используется инфракрасные тепловизионные камеры. Данные изображения обрабатываются в режиме реального времени. При изменении температуры контролируемой зоны происходит обнаружение БПЛА;

– Анализ радиолокационной сигнатуры. БПЛА обнаруживается по наличию их радиолокационной сигнатуры, которая генерируется, когда корпус БПЛА сталкивается с радиочастотными импульсами, излучаемыми радиолокационными системами.

– Обнаружение пакетной передачи данных. Радиочастотный спектр радиосвязи анализируется в режиме реального времени. Поток видео данных, модуляции и телеметрии перехватываются, декодируются. Это позволяет извлекать ценные данные, а также дает возможность для получения управления БПЛА.

Для повышения точности, отказоустойчивости, стабильности, позиционирования и дальности обнаружения БПЛА используют комбинированные методы обнаружения.

Для решения задач подавления БПЛА используются следующие способы:

– Акустическое воздействие. Поражение высокочастотной звуковой волной гироскопа приводит к дестабилизации полета БПЛА;

– Микроволновое воздействие. Происходит повреждение электроники БПЛА СВЧ излучением. Также микроволновое воздействие, в отличии от лазерного дает возможность одновременного уничтожения группы дронов.

– Использование так называемых «Противодронов». БПЛА-перехватчики оснащаются мощными двигателями и могут автоматически наводиться на дрон-нарушитель. БПЛА-перехватчик может быть оборудован сетью для поимки БПЛА-нарушителя.

– Хакинг и перехват управления БПЛА. Данный способ реализуется путем обнаружения и взлома шифрованного канала управления БПЛА. После чего происходит блокировка канала или перехват управления «на себя».

При проведении контртеррористических операций важную роль играют мобильные и быстро разворачиваемые комплексы противодействия БПЛА. Рассмотрим некоторые виды таких комплексов [3].

Носимый комплекс противодействия беспилотным летательным аппаратам «Пищаль-ПРО»

Рис. 1. Носимый комплекс «Пищаль-ПРО»

Носимый ручной комплекс «Пищаль-ПРО» предназначен для пресечения нахождения БПЛА в воздушном пространстве над зоной проведения специальных и контртеррористических операций путем подавления каналов связи, управления и навигации БПЛА с неподготовленных позиций.

В качестве ключевых особенностей можно указать сочетание высокой эффективности противодействия противоправному использованию БПЛА с безопасностью здоровья оператора. Также существует возможность работы устройства, как со стационарных позиций, так и в движении. Комплекс не требует специальной подготовки оператора и готов к боевому применению в масштабе времени, близкому к реальному. Стоит отметить, что вес «Пищаль-ПРО» составляет 3,5 кг, при этом дальность противодействия не менее 2000 метров [4].

Таблица 1

Технические характеристики «Пищаль-ПРО»

Частотные диапазоны постановки помех	Устройство обеспечивает одновременное воздействие на каналы связи, управления и навигационного обеспечения беспилотных летательных аппаратов
Напряжение электропитания	16 В
Емкость аккумуляторной батареи	10 А/ч
Тип формируемых помех	Шумоподобная, прицельная по направлению
Продолжительность непрерывной работы (на 2 АКБ)	не менее 1часа
Рабочий интервал температур	от –20 до +40 °С
Габаритные размеры (ШхВхД)	200х240х903 мм
Дальность подавления,	не менее, 2000м, при условии прямой видимости
Вес	не более 4 кг

Комплекс обнаружения и блокирования БПЛА «Персей–201»

Рис. 2. Комплекс «Персей–201»

Предназначен для повышения антитеррористической защиты правительственных зданий и территорий, аэропортов, объектов жизнеобеспечения, мест массового пребывания граждан.

Комплекс обеспечивает обнаружение и блокировку работы любого беспилотного устройства, включая микро и крупные БПЛА на дистанции до 4 км.

Блокиратор комплекса подавляет все радиочастоты управления беспилотниками, включая систему, которая позволяет беспилотникам использовать автопилот.

Комплекс является модульной системой, которая может использоваться для обнаружения, сопровождения подавления БПЛА в автоматическом или ручном режимах.

Для подавления используются направленные антенны и антенны круговой направленности в комбинации для ближнего и/или дальнего подавления.

Комплекс обеспечивает подавление всех коммерческих частот, которые могут использоваться для дистанционного управления БПЛА и GSNS (глобальной навигационной спутниковой системы). Могут использоваться антенны направленные или круговой направленности. Направленные антенны с высоким усилением размещаются на поворотно-наклонной платформе для сопровождения (отслеживания) перемещений БПЛА и передачи сигнала подавления в его направлении. Подавление может осуществляться автоматически с момента обнаружения БПЛА или в ручном режиме оператором.

Пользователь может выбирать между 2-мя режимами подавления – длительное/ручное или автоматическое подавление с момента обнаружения БПЛА радаром или тепловизором.

Антенная система комплекса обеспечивает обнаружение объектов площадью 0,006 м2 в радиусе до 6 км. При этом скорость сканирования будет равна 1 Гц. Система позволяет вести автоматическое слежение радаром за несколькими обнаруженными объектами. В целях повышения эффективности обнаружения «Персей-201» может быть оснащен камерой/тепловизором с приводом поворота/наклона и увеличительным объективом [4].

Таблица 2

Спецификации радара системы «Персей–201»

Радиус обнаружения микро–БПЛА	2км
Радиус обнаружения БПЛА	4км
Радиус обнаружения легкого воздушного судна	10км
Выходная мощность	2Вт
Сканирование по азимуту	360°
Частота сканирования	60 оборотов в минуту
Тип целей	микро–БПЛА, БПЛА, парапланы, легкие воздушные судна

Многофункциональный комплекс противодействия «Сапсан-Бекас»

Рис. 3. Мобильный комплекс «Сапсан–Бекас»

Осуществляет защиту охраняемых объектов и территорий от противоправных действий, совершаемых с использованием беспилотных летательных аппаратов. Также высокая мобильность комплекса «Сапсан–Бекас» дает возможность его использования в зонах проведения контртеррористических операций. В состав многофункционального комплекса противодействия «Сапсан-Бекас» входит подсистема радиотехнического обнаружения и пеленгации, подсистема активной радиолокации и оптоэлектронного сопровождения, подсистема радиоподавления.

Функциональной особенностью является работа многофункционального комплекса в масштабе времени, близком к реальному, а также обнаружение с применение средств РЛС, РТР, ОЭР и радиоэлектронное подавление (РЭП). Все средства обнаружения цели РЛС, РТР и ОЭР и воздействия объединены современным программным обеспечением с АРМ управления. Управление всем комплексом осуществляется 1 оператором [4].

Радиолокационная система «СМЕРЧ»

Рис. 4. Радиолокационная система «СМЕРЧ»

Данная система, как и комплекс «Персей-201» предназначена защиты зданий и территорий и штабов управления силами и средствами, задействованными при проведении специальных и контртеррористических операций от противоправных и диверсионных действий, совершаемых с помощью БПЛА.

Система «СМЕРЧ» позволяет сопровождать до 500 целей. Идентифицирует и классифицирует объекты, обеспечивает отрисовку контуров цели. Отслеживает малозаметные цели, в том числе в режиме радиомолчания. Радиолокационная система «СМЕРЧ» используется для защиты аэропортов, промышленных объектов, объектов государственной важности от атак БПЛА.

Система основана на использовании нового в радиолокации типа сигналов (ансамбль OFDM). Это позволило получить:

– разрешение по дальности порядка 4 см (ширина полосы 12.5 ГГц);

– устойчивость к помехам с полосой до 300 МГц;

– возможность построения дальностного портрета, классификации объектов;

– существенно большую дальность действия относительно РЛС на сверхкоротких импульсах (за счет большего коэффициента заполнения);

– динамический диапазон обеспечивает возможность одновременной работы с близкорасположенными и существенно удаленными объектами;

– совместимость с цифровыми фазированными антенными решетками, ввиду того, что для каждой несущей OFDM элементами антенны задается свое распределение фаз;

– нулевая минимальная рабочая дальность (прием ведется во время передачи, независимые антенны) [4].

Таблица 3

Технические характеристики радиолокационной системы «СМЕРЧ»

Чувствительность	140 дБм/Гц
Динамический диапазон	110 дБ
Максимальная скорость сканирования	11000 МГц/с
Сектор обзора пространства	по азимуту 360° по углу места 70°
Диапазон высот цели	до 4 км
Дальность обнаружения малоразмерной воздушной цели не менее	ЭПР до 0,02 м² ≥ 3600м ЭПР более 0,2 м² ≥7100м

Все выше сказанное показывает, что быстроразвивающаяся индустрия производства БПЛА дает широкие возможности их применения экстремистскими организация для совершения террористических актов.

Однако подводя итог применяемым методам и способам противодействия БПЛА, можно дать достаточно высокую оценку существующей в России возможности противостоять террористическим БПЛА. Существующие разработки позволяют создавать зоны, недоступные для современных управляемых дронов, используя системы подавления и перехвата вокруг них.

Литература

1. Атакующие БПЛА и системы противодействия им, обзор Электронный ресурс. Режим доступа: URL: http://savepearlharbor.com/?m=201506&paged=339 (дата обращения: 21.03.2021).

2. БПЛА Orbiter // Военное обозрение [Электронный ресурс], 17.06.2013. URL: https://topwar.ru/29512–bplaorbiter.html (дата обращения: 21.03.2021).

3. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В. Особенности обнаружения и распознавания малых беспилотных летательных аппаратов // Радиотехника. 2018. № 195. С. 235–243.

4. Духвалова И.Г., Ижогина Е.А. Открытый обзор продукции российских производителей специальных средств и техники (для комплексного обеспечения правоохранительной деятельности): Научно-технический информационный сборник. Вып. 2 (7). – М.: ФКУ НПО «СТиС» МВД России, 2020. – 88 с.

Потапов Иван Валерьевич,
orangeholland@icloud.com
ООО «Оксиджен Софтвер»

УСТАНОВЛЕНИЕ ФАКТА НЕЗАКОННОЙ ДЕЯТЕЛЬНОСТИ ТЕРРОРИСТИЧЕСКИХ ГРУППИРОВОК ПРИ ИССЛЕДОВАНИИ ДАННЫХ, ПОЛУЧЕННЫХ ИЗ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Повсеместное распространение Интернета и информационных технологий способствует постоянному развитию общества и коммуникации людей в повседневной, рабочей или учебной жизни. Широкий спектр Интернет-ресурсов и разного рода программного обеспечения позволяют выполнять практически любые задачи, имея под рукой смартфон или компьютер. Однако информационные технологии находятся и в арсенале незаконных экстремистских и террористических формирований. Далее в этой статье мы подробно рассмотрим основные виды преступной деятельности террористических ячеек в глобальной Сети, а также способы ее предотвращения и раскрытия.

Согласно докладу Управления Организации Объединенных Наций по наркотикам и преступности, существует шесть основных категорий методов использования сети Интернет в террористических целях. В числе этих методов:

– пропаганда (вербовка, радикализация и подстрекательство к терроризму);
– финансирование;
– обучение;
– планирование (в том числе координация с помощью мессенджеров);
– исполнение;
– кибератаки.

Основными задачами пропаганды являются насаждение радикальной идеологии, оправдание и реклама терроризма, призывы к насилию, вербовка сторонников и т. д. Вербовщики для достижения своих целей распространяют на форумах в Сети и в социальных сетях журналы, презентации, аудио, видеофайлы и изображения. Данные мультимедийные материалы воздействуют на широкую аудиторию, которая способна расти в геометрической прогрессии. Например, трудовые мигранты из мусульманских стран, живущие большими группами, более подвержены радикальной пропаганде. Таким образом, литература и информация, распространяемая в Интернете, оказывает влияние одновременно на широкую группу лиц.

В основном, подобного рода деятельность присуща больше «Исламскому государству», размещающему материалы под различными

«брендами», например «Аль-Фуркана», ориентированным на уже существующую аудиторию или «Аль-Хайята» – на зарубежную. «Аль-Каида», также использующая всемирную сеть, не имеет сравнимых ресурсов для распространения радикальных идей среди мусульман, однако их деятельность в Сети представляет серьезную угрозу. (Александр Крупнов, Аналитический доклад «Исламское государство». Пропаганда группировки и механизмы ее распространения., Москва, 2017).

С помощью Интернет–ресурсов и сервисов коммуникации также осуществляется финансирование деятельности террористических и экстремистских ячеек. Существует несколько способов получения денежных средств незаконными формированиями. Первый из них – открытые просьбы о переводе пожертвований, обычно осуществляемые посредством размещения соответствующих сообщений в социальных сетях, мессенджерах или форумах в Даркнете. Второй – своеобразная электронная коммерция, которая заключается в продаже запрещенных товаров на торговых площадках. Вырученные средства идут на покупку оружия, поддельных документов и различного оборудования для подготовки и исполнения террористических актов.

Подготовка и радикализация членов экстремистских и террористических организаций происходит и на альтернативных дистанционных площадках в Интернете. Так, журнал «Inspire», по некоторым предположениям, является руководством «Аль-Каиды» для мусульман по подготовке к джихаду в бытовых условиях. Данное интернет–издание было переведено на множество языков, в том числе на русский. Таким образом, крупные группировки оказывают влияние на страны Европы, принимая участие в эскалации локальных конфликтов, например, на Северном Кавказе.

Распространение подобных материалов представляет собой опасность в силу угрозы массовой радикализации сообщества и, как следствие, увеличения количества террористических актов.

В рамках подготовки к исполнению и собственно исполнения актов терроризма, участники незаконных формирований осуществляют коммуникацию посредством программ для мгновенного обмена сообщениями или почтовых сервисов. Для распространения запрещенных материалов и получения финансирования необходим доступ к глубинному сектору Интернета, который возможно получить с помощью, например, Tor Browser. В качестве же примеров программного обеспечения, которое может быть использовано радикальными группировками для координации действий во время подготовки и совершения террористических актов, можно привести Telegram, Signal, Wickr Me, VIPole, Viber, Unigram, TamTam и др.

Хотя информационные технологии активно используются террористическими и экстремистскими группировками для достижения

своих целей, эти же технологии могут помочь в предотвращении, пресечении террористической деятельности и сборе доказательств для привлечения членов незаконных бандформирований к ответственности. Безусловно, предотвращение пропаганды терроризма и вербовки сторонников – это затратные меры, дающие только краткосрочный результат, так как удаленные группы в социальных сетях и заблокированные веб-ресурсы в Интернете могут быть созданы заново. Тем не менее, отсутствие притока радикально настроенных мигрантов из-за рубежа не гарантировано, а следовательно, и отсутствие террористических актов – тоже.

В свою очередь, пресечение террористических актов на стадии подготовки и сбора цифровых доказательств для привлечения членов и глав незаконных формирований обеспечивает большую уверенность в безопасности граждан. На данном этапе развития информационных технологий, выполнению этих задач способствует использование специального программного обеспечения для извлечения и анализа данных из персональных компьютеров. Несмотря на повсеместное распространение смартфонов, основная деятельность террористических организаций в Интернете происходит с использованием преимущественно персональных компьютеров, так как требует более серьезных мощностей для входа в глубинный сектор Интернета, изготовления и распространения графических материалов и видеороликов. Именно поэтому на современном этапе наиболее приоритетной целью сбора цифровых доказательств террористической и экстремистской деятельности являются персональные компьютеры и ноутбуки подозреваемых лиц.

Возможность извлечения и анализа информации из этих устройств обеспечивают программные инструменты бренда «Мобильный Криминалист». Модуль «МК Скаут», доступный в программах «Мобильный Криминалист Эксперт» и «Мобильный Криминалист Десктоп», осуществляет поиск данных не только на запущенных системах под управлением Windows, macOS и GNU/Linux, но и образах жестких дисков с файловой системой NTFS в формате e01, а также образах файловой системы ПК в форматах ZIP и AD1 (Access Data).

Данное программное обеспечение позволяет решать ключевые задачи расследования террористической деятельности:

1) Установление факта посещения веб-ресурсов в Интернете и его глубинном секторе.

«Мобильный Криминалист Скаут» поддерживает извлечение информации из популярных веб-браузеров для всех операционных систем: Google Chrome, Mozilla Firefox, Opera, Safari, Chromium, Microsoft Edge и Internet Explorer. В результате, исследователю на анализ попадают история посещений веб-страниц, закладки, загрузки, данные веб-форм, профили, а также пароли и токены для авторизации в сторонних сервисах. Отдельно

стоит отметить получение информации Tor Browser: с помощью рассматриваемого программного обеспечения возможно изучить историю посещения веб-страниц, закладки, данные веб-форм, а также логины, пароли и токены для авторизации в различных приложениях или Интернет-ресурсах, включая незаконные торговые площадки (например, Hydra) и анонимные почтовые сервисы, доступные исключительно в Tor, например, secMail.

2) Выявление фактов коммуникации внутри террористических ячеек с использованием сервисов для мгновенного обмена сообщениями.

Модуль «Скаут» обладает возможностями получения сведений из настольных версий большинства популярных мессенджеров, в том числе и наиболее защищенных: Telegram for macOS, Signal, Wickr Me, VIPole, Viber, GroupMe, Unigram, TamTam и др. Так, программное обеспечение получает из сервисов для мгновенного обмена сообщениями переписки пользователя, информацию о личных и групповых чатах, данные о контактах, звонках (если функция поддерживается приложением), опросах, заметках, а также об учетной записи. Анализ указанных категорий сведений позволяет не только доказать факт коммуникации внутри незаконных бандформирований и привлечь участников к уголовной ответственности, но и своевременно получить информацию о готовящихся террористических актах и принять меры для их пресечения.

3) Обнаружение на устройствах подозреваемых материалов, запрещенных к распространению на территории Российской Федерации.

Помимо данных различных приложений модуль также исследует файловую систему персонального компьютера или образа. Исследователь имеет возможность оперативно проанализировать аудио, видео, графические материалы, документы и другие файлы на изучаемом цифровом источнике. Кроме того, программа с помощью встроенных нейронных сетей самостоятельно проводит категоризацию изображений, определяя угрозы на них, и распознает лица на фотографиях, что позволяет сэкономить время при анализе собранных цифровых доказательств и обнаружить запрещенные материалы, используемые для пропаганды терроризма, радикализации населения или подготовки к совершению террористических актов.

В заключение следует сказать, что на сегодняшний день не существует какого-либо универсального метода противодействия террористической активности в Интернете. Предотвращение пропаганды, осуществляемое с помощью сотрудничества с социальными сетями и регуляторами, безусловно, эффективный способ, однако не несет долгосрочного результата. В то же время, извлечение и анализ данных с помощью специального программного обеспечения непосредственно из устройств подозреваемых позволяет пресечь планируемые террористические акты и привлечь участников незаконных

бандформирований к ответственности, что, тем не менее, не снижает количество пропагандистских материалов в Сети. На данный момент рассмотренная проблема является крайне важной в связи с большей вовлеченностью в Интернет не только простых граждан, но и крупных мировых террористических группировок. На наш взгляд, для достижения наилучшего результат оптимальным способом противодействия экстремизму и терроризму является комбинация существующих методов.

Литература

1. Александр Крупнов, Аналитический доклад «Исламское государство». Пропаганда группировки и механизмы ее распространения. Москва, 2017. URL: https://www.mrsu.ru/ru/getfile.php?ID=84596
2. Доклад управления ООН по наркотикам и преступности, 2013, URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf
3. Молодые мигранты становятся мишенью для вербовщиков террористических организаций, 2020 URL: https://media–mig.ru/news/molodye–migranty–stanovjatsja–mishenju–dlja–verbovshhikov–terroristicheskih–organizacij/
4. Онлайн-журнал «Аль-Каиды» переведен на русский, 2011, URL: https://inosmi.ru/politic/20110519/169562816.html

Пьянников Владимир Игоревич,
piano.88@mail.ru
Академия управления МВД Российской Федерации

УПРАВЛЕНИЕ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН ПРИ ВОЗНИКНОВЕНИИ ТЕРРОРИСТИЧЕСКОЙ УГРОЗЫ КАК ОДНОГО ИЗ ВИДОВ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ СОЦИАЛЬНОГО ХАРАКТЕРА

Аннотация: В статье рассматривается управление органами внутренних дел при возникновении чрезвычайных ситуациях
Ключевые слова: терроризм, экстримизм, чрезвычайная ситуация.

Чрезвычайная ситуация социального характера – это обстановка на определенной территории, сложившаяся в результате опасного социального явления, которое повлекло или может повлечь за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий

жизнедеятельности людей. Одним из видов чрезвычайных ситуаций социального характера является как терроризм так и террористические акты.

Терроризм – один из вариантов тактики политической борьбы, связанный с применением идеологически мотивированного насилия. Суть терроризма-насилие с целью устрашения.

При возникновении террористической угрозы, противодействие оказывают все сотрудники правоохранительных органов, большая часть возложена на сотрудников органов внутренних дел (далее – ОВД).

Сфера охраны правопорядка в ракурсе предупреждения, пресечения, непосредственного противодействия и устранения последствий чрезвычайных ситуаций (далее – ЧС) социального характера является комплексной и динамичной, а потому требует стабильного совершенствования, которое возможно лишь при эффективном и детализированном нормативно–правовом регулировании и соответствующем информационно–аналитическом обеспечении.

Нормативно-правовые аспекты регламентации деятельности ОВД Республики Казахстана (далее – РК), в т. ч. во взаимодействии с иными органами, уже нашли свое отражение в работах казахстанских авторов. В связи с чем, имеется необходимость обратиться к непосредственному организационно-правовому регулированию информационно-аналитического обеспечения функционирования ОВД РК при ЧС социального характера в контексте управленческого воздействия и на сам процесс противодействия таковым ситуациям, и на деятельность соответствующих правоохранительных органов.

Известный исследователь В.Г. Афанасьев справедливо подчеркивает, что управляющая и управляемая системы не могут существовать без информации. Именно отлаженная систематичность информационно-аналитического обеспечения ОВД, даст возможность эффективно обеспечить все виды управленческой деятельности, организовать качественную связь, возникающую между различными звеньями системы управления, а также решать текущие проблемы в процессе осуществления противодействия чрезвычайным ситуациям социального характера (в том числе и терроризма) отделами и управлениями органов внутренних дел Казахстана.

На основании анализа научных работ относительно управленческого и организационного обеспечения функционирования правоохранительной службы, механизм информационно-правового механизма публичного управления деятельностью ОВД РК в целом можно определить как комплекс правовых, технологических, организационных средств, обеспечивающих процесс сбора, получения, обработки, распространения, анализа и применения информационных ресурсов, которые необходимы для осуществления определенных законом задач и функций этого органа.

Следует отметить, что вопросы информационно–аналитического обеспечения ОВД утвержден приказом Министра внутренних дел Республики Казахстан от 29 июля 2014 г. № 477 (положение 15).

При этом следует согласиться с мнением о том, что информационно-аналитическое обеспечение ОВД РК представляет собой систему правовых, организационных, технологических и технических средств, мероприятий и методов, гарантирующих в процессе управления и деятельности структуры информационные взаимосвязи ее элементов (объектов и субъектов) путем эффективного построения информационных массивов знаний и баз данных.

Построение структуры информационно-аналитического обеспечения обусловлено необходимостью повышения эффективного уровня деятельностью ОВД, благодаря чему обеспечивается:

– оперативное предоставление информации в подразделения ОВД от служб со сходным функционалом и в обратном направлении;

– способствование сокращению технологического цикла;

– определение путем анализа и оценки возможности изменений масштаба работы ОВД РК при ЧС социального характера;

– анализ и обобщение ранее полученных результатов противодействия ЧС социального характера, что позволит сосредоточить на определенных участках работы основные усилия ОВД РК;

– выявление наиболее рациональных путей моделирования распределение ресурсов и сил ОВД РК;

– установление направлений корректирования методов и форм непосредственного функционирования ОВД РК при ЧС социального характера, а также взаимодействия последних с иными органами и службами, наделенными сходным потенциалом.

Результаты информационно-аналитического обеспечения являются особенно важными для сотрудников ОВД РК, где от оперативности и скорости принятия управленческого решения нередко зависит жизнь большого количества людей, если речь идет о предотвращении или непосредственном устранении последствий ЧС социального характера, в т. ч. характеризующихся масштабностью и остротой течения. В наше время для решения этой проблемы уже недостаточно только традиционных методов, сложившихся, как правило, на профессиональном опыте и интуиции лица, принимающего решение. Требуется привлечение таких информационных технологий, которые в состоянии обеспечить автоматизацию процессов принятия решения. Именно с помощью современных информационных технологий можно ввести замкнутый контур управления, при котором субъект управления, принимая решение для объекта его исполнения, сможет продолжать отслеживать и своевременно вмешиваться в исполнение принятого решения.

При этом в зависимости от территориального подчинения, информационно-аналитическое обеспечение функционирования ОВД РК в контексте противодействия ЧС социального характера в том числе и терроризму осуществляется на трех уровнях.

Первый уровень – надотраслевой – предусматривает регулирования информационного обмена в процессе непосредственного выполнения функций ОВД РК и структур со смежным функционалом, прежде всего – в рамках взаимодействия упомянутого органа с Министерством по чрезвычайным ситуациям РК и Комитетом национальной безопасности РК.

Комплекс информационных учетов на этом уровне формируют:

а) банк криминологической информации о резонансных и нераскрытых тяжких преступлениях, в т. ч. посягающих на территориальную целостность и государственное устройство Республики Казахстан; о чрезвычайных происшествиях в целом; об инструментах совершения преступлений; о лицах определенных категорий: ранее совершавших сходные преступления; объявленных в розыск; осужденных за преступления, связанные с финансированием терроризма; лиц, причастных к наркоторговле, склонных к совершению преступных деяний, посягающих на интересы страны; организаторов и членов криминальных группировок, киллеров; неизвестных больных и неопознанных трупов; без вести пропавших;

б) статистический банк информации, в котором содержатся данные о состоянии преступлений, сопутствующих чрезвычайным ситуациям социального характера, посягающих на территориальную целостность и государственное устройство Республики Казахстан, и результаты борьбы с ними;

в) банк справочно-оперативной информации, в котором сохраняются данные дактилоскопического и алфавитного учетов ранее судимых лиц;

г) банк регистрации паспортных данных граждан;

д) банк специализированной информации;

е) банк данных о регистрации транспорта;

ж) банки данных управленческо-административного назначения;

з) банк регистрации огнестрельного оружия;

и) банки данных специальных фондов и архивов;

к) банки данных специального назначения структурных служб.

Второй уровень – базовый ведомственный – объединяет информационные структуры ОВД РК общеведомственного назначения и отраслевых подразделений МВД РК, в частности, Нацгвардии и МПС РК.

На этом уровне формируется информация, которая применяется при планировании, анализе, принятии управленческих решений и проведении в рамках Республики Казахстан поисково-оперативных, следственных и других спецмероприятий по противодействию чрезвычайным ситуациям социального характера.

Третий уровень – региональный – включает информационные учеты, являющиеся элементами общеведомственных информационных систем, и реализуется службами ОВД РК на уровне акиматов.

На основании вышеизложенного, следует, что в существующим опыте практического внедрения организационного механизма функционирования информационно-аналитических систем, в деятельности ОВД РК есть пробелы такие как:

1) дублирование сбора и многократная переработка одних и тех же данных различными структурными службами и на разных уровнях;

2) несогласованность в формировании и внедрении информационных банков данных;

3) слабая информационная взаимосвязь между регистрационно–учетными, оперативно-розыскными и справочными фондами различных служб и ведомств, подчиненных как одному министерству (МВД РК, включая МПС и Нацгвардию Казахстана), так и различным министерствам со сходным функционалом (включая МЧС РК и Комитет национальной безопасности Казахстана);

4) недостаточная достоверность и полнота данных в связи с нарушением порядка и сложностями с обменом данными между подразделениями в пределах одного ведомства или различными правоохранительными органами со сходным функционалом;

5) отсутствие должного и реального информационного взаимодействия между заинтересованными департаментами, органами и учреждениями;

6) латентность, представленная в форме укрытия преступлений от статистической государственной отчетности (неаргументированный отказ в возбуждении уголовных дел и приостановление, переквалификация преступлений, наиболее часто совершаемых при ЧС социального характера, с тяжких на менее тяжкие; нефиксирование сообщений о преступлениях и др.), что вызывает искривление фактического состояния дел;

7) несвоевременное поступление к лицам служебно-оперативной информации из-за несовершенной технологии представления информации в банки данных и неиспользования новых средств связи и компьютерной техники;

8) несовершенное организационно-кадровое обеспечение информационных отделов ОВД РК в регионах и в структурных службах;

9) устаревшие технические комплексы ОВД РК в регионах;

10) неурегулированность и несовершенство законодательной базы

Причины такой ситуации заключаются в том, что, с одной стороны, существуют недостатки в постановочных разработках систем, а с другой – наличествует реальная оторванность определенных потребителей информации (практических сотрудников ОВД РК) от банков данных, невозможность или неудобство прямого доступа к информации, и потому – их незаинтересованность в поддержании информационных подсистем в надлежащем состоянии.

Литература

1. Соспинов М.Н. К вопросу о методах выработки и исполнения управленческих решений в органах внутренних дел // Пробелы в российском законодательстве. 2012. № 1. С. 216–219.

Сайбель Алесей Геннадиевич,
saybel_ag@mail.ru
Санкт-Петербургский Университет МВД России

ТЕХНИЧЕСКИЕ РЕШЕНИЯ ДЛЯ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ АППАРАТНЫХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ФИНАНСИРОВАНИЯ ПРОТИВОПРАВНЫХ ДЕЯНИЙ

Аннотация: Представлены результаты анализа применимости технологий компьютерной экспертизы для исследования современных технических средств дистанционного банковского обслуживания.

Технология исследования конкретного радиоэлектронного устройства зависит от его конструктивных и структурно-функциональных особенностей, технического состояния, а также поставленных перед экспертизой вопросов. При этом эксперт решает исключительно технические вопросы, а бремя юридической интерпретация полученных ответов лежит на следственных органах и других участниках судебного процесса [1–3].

Достаточно новым объектом экспертного исследования являются современные индивидуальные средства дистанционного банковского обслуживания (ДБО), в качестве которых в настоящее время используются пластиковые карты и имитирующие их специализированные или универсальные устройства. Существенной особенностью таких средств ДБО является сочетание качеств, позволяющих отнести данный класс устройств к объектам компьютерной экспертизы (КЭ).

Карты с магнитной полосой отнесены к объектам КЭ уже при разработке и создании Автоматизированного рабочего места для проведения криминалистических экспертиз электронных носителей информации [4]. В ходе организованной СТиС МВД России опытно–конструкторской работы «Карта» разрабатывались технические решения по исследованию чиповых смарт-карт. В современных условиях смарт–карты и иные устройства (ИУ), используемые для дистанционных платежей, выступают в качестве объектов криминалистического исследования не только в связи с противоправными действиями, направленными на хищение средств со счетов частных лиц, но и в рамках расследований финансирования террористической и экстремистской деятельности.

Трансграничное материально-финансовое обеспечение противоправной деятельности, направленной на дестабилизацию положения в стране, против политической системы государства и на раскачивание устоев общества, осуществляется тремя основными путями: завозом через границу наличных средств, переводом платежей через систему межбанковского обмена информацией или с использованием криптовалюты, а также завозом через границу пластиковых карт.

Пластиковые карты не относятся к валютным ценностям и не подлежат внесению в таможенную декларацию, поэтому третий вариант представляет интерес, поскольку одновременно непротивоправен и сложно отслеживаем.

В меньшей степени чем десять лет назад, но по-прежнему остается актуальным вопрос исследования пластиковых карт в рамках расследований мошеннических деяний, направленных на получение доступа к банковским счетам частных граждан на основе применения классических атак, направленных на карту или ее реквизиты:

– копирование магнитной полосы карты (*skimming*).

– заедание карты в считывающем устройстве (ридере) с целью ее дальнейшего незаконного изъятия (*jamming*, *trapping*).

– подмена или присвоение карты незаметно для держателя после выполнения операции на банкомате (*swapping*).

– фальшивые банкоматы.

– кибератака – информация о реквизитах карты присваивается путем незаконного доступа в систему банкоматов или к каналам связи.

Изначально платежные карты выступали в роли средства идентификации личности владельца банковского счета, с которого осуществляется оплата товара или услуги. Надежность идентификации определялась уникальностью экземпляра карты и дополнительной возможностью подтвердить личность владельца сверкой росписей, выполненной предъявителем и представленной на обороте карты. Подделка карт затруднялась эмбоссированием, а позднее дополнительными элементами защиты в виде голограмм и лазерного нанесения текста. Добавление магнитной полосы повысило оперативность использования карт, но снизило тщательность контроля внешнего вида и создало новые варианты получения незаконного доступа к средствам банковских счетов на основе хищений карт, купюр при выполнении действий с банкоматом [5], а также идентифицирующих данных карты, позволяющих изготовить ее функциональную копию.

В последствие смарт-карты расширили свои возможности до полноценного микрокомпьютера, позволяющего осуществлять сбор, хранение, обработку и передачу информации, кодирование и шифрование данных, контактное и дистанционное взаимодействие с платежными терминалами и системами контроля и управления доступом.

Интеграция функций смарт-карт в телекоммуникационные устройства повысила удобство их использования, а достижения микроминиатюризации позволили встраивать смарт–элементы платежных карт в предметы быта, элементы одежды и аксессуары, бижутерию и ювелирные украшения, а также имплантировать специализированные микромодули в биологические объекты.

Контактное и бесконтактное взаимодействие современной пластиковой карты или устройств, имитирующих их функционал, осуществляется встроенной микропроцессорной системой, нагруженной на приемно-передающую антенную систему, которая также задействуется для формирования питающих напряжений, необходимых для работы электронных компонент в режиме бесконтактного взаимодействия, за счет накачки от внешнего источника.

Такие устройства позволяют осуществлять передачу и прием сигналов и данных для выполнения юридически значимых действий и других целей, в зависимости от предустановленного и специально установленного программного обеспечения.

Вместе с тем до сих пор есть регионы мира, в том числе в некоторых штатах США, в которых отсутствуют современные средства ДБО и для осуществления платежей с использованием банковских карт применяются импринтеры.

С точки зрения проведения компьютерной экспертизы особенностями смарт-карт являются:

– стандартные геометрические параметры;

– стандартные протоколы обмена данными;

– многообразие вариантов представления пользовательской информации;

– наличие процедур авторизации пользователя.

Для иных устройств, имитирующих смарт-карты, геометрические параметры могут быть произвольными.

Для всестороннего исследования объектов указанной группы в рамках выполнения опытно-конструкторской работы разработан Аппаратно-программный комплекс «Карта-М», который в 2020 году успешно прошел Государственные испытания. Комплекс позволяет:

– с высокой надежностью оперативно создавать большой двоичный объект в качестве информационной копии электронных носителей информации (ЭНИ), в роли которых выступают пластиковые карты, при этом количественные и качественные характеристики ЭНИ не изменяются, что имеет решающее значение для обеспечения законной силы результатов процедуры судебной экспертизы;

– обрабатывать большой двоичный объект с использованием специального программного обеспечения для получения ответов на вопросы, поставленные перед экспертом;

– формировать итоговое экспертное заключение.

Для формирования описаний исследуемых карт в составе комплекса предусмотрено использование сканера со специализированным трафаретом, позволяющим удобно размещать объекты экспертизы в восьми ячейках, фиксированное положение которых в поле сканирования позволяет автоматизировать процесс формирования изображений для включения в состав большого двоичного объекта, описывающего каждую карту.

Ячейки для размещения пластиковых карт имеют размеры, соответствующие Международному стандарту ISO-7810, форма каждой ячейки имеет боковые расширения для удобства извлечения карт.

Кроме изображений исследуемой карты в состав большого двоичного объекта входят наборы данных, считанные с магнитной полосы, а также с встроенного микропроцессора (при его наличии) с использованием контактного и бесконтактного считывателей.

В качестве считывателей информации с магнитной полосы и чипа использованы MSR-206U, Omnikey 3121 и Omnikey 5422.

АПК «Карта-М» функционально обеспечивает:

1) чтение 1, 2, 3 дорожек карт с магнитной полосой, соответствующих стандартам ISO 7810, ISO 7811;

2) подключение и чтение чиповых смарт-карт, соответствующих стандартам ISO 7816, EMV 2000;

3) подключение и чтение чиповых смарт-карт с двойным интерфейсом (proximity) и комбинированных карт, соответствующих стандартам ISO 7810, ISO 7811, ISO 7816, ISO 14443;

4) фотофиксацию носителей информации и последующее документирование процесса исследования;

5) подключение и чтение наиболее распространенных типов бесконтактных пластиковых карт (стандарта ISO 14443) для их последующего исследования;

6) подключение ИУ, использующих для осуществления платежных операций технологии NFC и MST.

Международные стандарты, описывающие структуру протоколов обмена информации и представления данных, предоставляют банкам широкие возможности по определению пользователем смысловой нагрузки передаваемых бит информации. Поэтому карты разных банков позволяют получить из них разные наборы данных, общим для которых является информация о номере карты и сроке действия.

Проведенные пробные тестирования доступных устройств, имитирующих функции банковских карт, показали, что производители по-разному используют возможности протоколов обмена. Меньше всего данных позволяет получить G-Pay.

Особенностью исследования смартфонов, использующих для осуществления платежных операций технологии NFC, является несовпадение номеров исходной карты и созданной на ее основе виртуальной. Срок действия виртуальной карты также не совпадает со сроком действия реальной карты. При этом отображаемое на экране мобильного приложения изображение карты не является фотокопией привязанной карты, а представлено в виде аватара, предоставляемого банком по номеру регистрируемой карты. Таким образом извлечь из смартфона в рамках криминалистической компьютерной экспертизы сведения о держателе карты, зарегистрированной в платежном приложении, не представляется возможным. Доступный эксперту номер виртуальной карты позволяет [6] установить банк–эмитент, через запрос которому может быть установлен держатель карты.

В ходе проработки архитектуры и состава АПК «Карта-М» был выполнен анализ современных периферийных устройств считывания информации с пластиковых карт. В качестве перспективного образца был отобран и исследован комбинированный считыватель карт HCC-110 (Китай). Устройство позволяет обеспечить взаимодействие компьютера с пластиковыми картами с магнитной полосой, контактными и бесконтактными чиповыми картами, а также с sim-картами по интерфейсу USB и бесконтактно. Компактность (180 г) и универсальность считывателя

позволяют удобно использовать его для широкого круга экспертных задач компьютерной экспертизы. Предоставляемый производителем SDK позволяет встраивать прилагаемое программное обеспечение в исследовательские комплексы. Однако протокол взаимодействия с устройством производитель не предоставляет, что не позволяет использовать устройство в качестве периферийного для самостоятельно разрабатываемых АПК; по отзывам пользователей надежность считывателя составляет величину менее 50%; на территории Российской Федерации нет официального представительства производителя, купить устройство можно только через сетевые торговые площадки.

Литература

1. Зубаха В.С., Усов А.И., Саенко Г.В., Волков Г.А., Белый С.Л., Семикаленова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. – М.: ГУ ЭКЦ МВД России, 2000. – 65 с.
2. Шелудченко В.И. Технико–криминалистические средства и методы собирания компьютерной информации // Материалы Всероссийского межведомственного семинара. Белгород: МВД РФ, 2002. – С. 205–207.
3. Айков Д., Сейгер К., Фопсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. /Пер. с англ. В.И. Воропаева и Г.Г. Трехалина. – М.: Мир, 1999.
4. Голубев В.А., Зайцев И.Е., Сайбель А.Г. Автоматизированное рабочее место для проведения криминалистических экспертиз электронных носителей информации. Патент на изобретение РФ № 2297664 от 20.04.2007.
5. Баркалов Ю.М., Сайбель А.Г. Информационно-безопасностная модель оборудования дистанционного банковского обслуживания // Охрана, безопасность, связь. 2017. № 1-1. С. 27–33.
6. Голубев В.А., Зайцев И.Е., Сайбель А.Г. Облачный сервис и система для проведения компьютерных судебных криминалистических экспертиз карт с магнитной полосой. Патент на изобретение РФ № 2517235 от 27.05.2014.

Бекежанова Азиза Биржановна,
aziza.bekezhanova@,mail.ru
Барнаульский юридический институт МВД России

Тимофеев Виктор Владимирович,
v.v.timofeev@bk.ru
Барнаульский юридический институт МВД России

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ПОИСКОВОЙ ТЕХНИКИ В БОРЬБЕ С ТЕРРОРИЗМОМ

Одной из основных задач в борьбе с преступлениями террористической направленности является формирование научно обоснованных рекомендаций использования поисковой специальной техники. Основная проблема состоит в снижении антитеррористической защищенности объектов вследствие высокой стоимости поисковой техники, следовательно, ряд групп досмотровой техники не закупаются. Кроме того, контролеры, чаще всего, при массовом скоплении людей, недостаточно тщательно осуществляют досмотр через досмотровую зону. Очевидно, подобная ситуация является крайне нежелательной.

Особая роль при обеспечении общественной безопасности, предупреждении подготовки и совершения террористических актов принадлежит досмотровой технике.

В основе принципа своего действия технические средства досмотра багажа и граждан в основном используют физические контрасты объекта поиска на фоне укрывающей среды, являющейся преимущественно неметаллической, также они применяются на объектах транспортной инфраструктуры при проверке грузов, почты, бортовых припасов, а также перевозимых гражданами личных вещей. Второй группой досмотровой техники являются стационарные рентгено-телевизионные установки (интроскопы), позволяющие выявлять металлические объекты поиска в условиях наличия существенного количества металла в укрывающей среде. В качестве объекта исследования для детекции они используют данные, получаемые в виде теневого изображения объектов после просвечивания в установке, либо отраженное рентгеновское излучение. Дополнительное повышение контрастности формируемого на мониторе изображения происходит с использованием средств цифровой обработки сигнала, поступающего на приемную часть установки от объекта досмотра. По своим функциональным возможностям они бывают одноракурсными и многоракурсными. Вторые более точно определяют не только теневой контур объектов поиска, но и входе обработки сигналов отклика от досматриваемого объекта, создают объемное изображение его внутреннего объема и предметов, находящихся в нем.

Третья группа досмотровой техники представлена томографическими установками, функционирующими на основе эффекта магнитно-резонансной томографии. Они позволяют досматривающим лицам выявлять жидкости, металлы, пластики и керамику в багаже и ручной клади пассажиров, идентифицируя объекты поиска по характерному для их материалов отклику на облучение электромагнитным сканирующим сигналом. Четвертой группой досмотрово-поисковой техники являются портативные интроскопы, представляющие собой, преимущественно, устройства для использования в условиях оперативной обстановки, в том числе на месте происшествия, связанного, либо имеющего отношение к готовящемуся террористическому акту. В отношении принципа действия эта группа технических средств поиска аналогична второй, имеются лишь особенности ее конструктивного исполнения, связанные с требованиями минимизации массо-габаритных показателей изделия и его моноблочного исполнения. Указанные изделия широко используются для проверки бесхозного багажа, предметов ручной клади в пассажирской зоне аэропортов или на борту самолета для их бесконтактного досмотра. В пятую группу можно объединить газоаналитическое оборудование, ориентированное на поиск взрывчатых веществ и наркотиков. В конструктивном отношении газоанализаторы могут быть выполнены стационарно – для использования на объектах транспортной инфраструктуры и проходных предприятий, связанных с производством и использованием взрывчатых веществ. Газоанализаторы в портативном конструктивном исполнении используются при досмотре помещений, предназначенных для проведения массовых мероприятий, в ходе проведения обысков.

По эффективности выявления объектов поиска наиболее результативным будет являться сочетание досмотрово-поисковых технических средств различного назначения, поскольку на момент организации поиска неизвестно, какой именно объект необходимо обнаружить.

Немалую по значению роль играет и тактически верное использование имеющихся в распоряжении ОВД технических средств контроля и досмотра. Так, в ситуации, близкой к идеальной по эффективности поиска для досмотра должны совместно применяться металлодетекторы, интроскопы, газоанализаторы. Как известно, металлодетекторы могут быть двух основных видов: стационарные (арочные) и портативные (ручные). Их выбор осуществляется, исходя из особенностей поисковой ситуации.

Стационарные металлодетекторы устанавливаются в местах, где осуществляется досмотр лиц при входе в помещение или на закрытую от посторонних лиц территорию. Примерами являются модельные ряды металлодетекторов «Паутина», «Поиск», «Ника» и прочие другие, которые

также имеют возможность негласного досмотра лиц (например, при скрытой установке в дверных проемах, проходах и т. д.).

Ручными металлодетекторами может осуществляться поиск металлических предметов в одежде, ручной клади и прочих местах и вещах. Наиболее распространенным является модельный ряд портативных металлодетекторов «Сфинкс».

Принцип организации поиска с использованием современного интроскопа достаточно прост. Объект, подлежащий досмотру, движется по транспортеру и, после помещения его внутрь интроскопа, облучается рентгеновской трубкой. В зависимости от толщины и материала объекта в нем теряется часть энергии излучения. Остаточная энергия регистрируется специальными детекторами, работающими на просвет или отражение, и преобразуется в электрические сигналы, которые впоследствии визуализируются. Чем более плотный багаж, тем меньше излучения попадает на детекторы. В конечном итоге интроскоп генерирует проекцию досматриваемого объекта, которая отражает его внутреннюю структуру.

Кроме вышеописанной досмотровой техники для досмотра людей могут применяться газоанализаторы, позволяющие выявить микрочастицы взрывчатых и наркотических веществ, которые находятся на теле человека, проходящего через створ детектора. Современные газоанализаторы – детекторы взрывчатки, работают по технологии спектрометрии, изучающей подвижность ионных частиц, либо используют специализированные детекторы – газовые сенсоры. Она отличается тем, что обеспечивает достаточно высокую точность контроля.

Следующая группа поисковой техники – досмотровые зеркала, эндоскопы, видеокамеры относятся к средствам визуального контроля. Досмотр транспортных средств, колесных арок осуществляется с помощью досмотровых зеркал. Данная досмотровая техника используется для обследования мест, осмотр которых невооруженным глазом практически невозможен, в целях обнаружения предметов, свободный оборот которых запрещен, а также обеспечения безопасного режима на объектах транспортной инфраструктуры.

Наряду с многообразием технических средств досмотра человека, транспорта, багажа, остаются актуальными и нерешенными некоторые проблемы в области их применения.

Проблема недостаточно профессиональной работы досматривающих лиц может быть решена привлечением на одну зону досмотра контролеров из числа высококвалифицированных и ответственных кадров, а также своевременным повышением квалификации всего имеющегося персонала.

В большинстве случаев, как было отмечено выше, поисковая техника обладает достаточно высокой стоимостью. Соответственно, обеспечение приобретения современного оборудования – это один из вариантов решения указанной проблемы.

Для достижения необходимых результатов в борьбе с терроризмом, считаем необходимым внедрять новое оборудование с современными технологиями обнаружения оружия, взрывчатых веществ и других предметов, свободный оборот которых ограничен. В то же время повысить эффективность имеющихся средств досмотра и поиска возможно путем их комплексного использования, как на рубеже контроля, так и при проведении обысков.

Литература

1. Полоскун Ю.М., Андреев К.Н. Технические средства таможенного контроля. – М.: Юрайт, 2010 . – С. 40–57.
2. Синютин, Ю.В. Поисково–досмотровая техника, используемая сотрудниками органов внутренних дел Российской Федерации в период подготовки и проведения массовых мероприятий // Проблемы и совершенствование методологии специальной подготовки правоохранительных органов в период проведения крупных общественно–политических и спортивных мероприятий, в том числе чемпионата мира по футболу FIFA 2018 года. Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя. – М., 2018. – С. 136–144.
3. Досмотровая техника. URL: Технические средства досмотра багажа и ручной клади (1cpbo.ru) (дата обращения: 19.03.2021).
4. Баумтрог В.Э., Каширский Д.Ю., Тимофеев В.В., Технический аспект содержания определения «специальная техника органов внутренних дел». Естественные и технические науки, 2019. – № 1 (127) – С. 149–151.
5. Имамова В.Р., Тимофеев В.В. Визуализация информации об объекте поиска с помощью металлоискателя годографа. Вестник Барнаульского юридического института МВД России. 2017. № 1 (32). С. 226–227.
6. Тимофеев В.В, Кирюшин И.И. Реализация современных технологий образовательного процесса по дисциплине «Специальная техника ОВД» с использованием магнитного томографа «ЗОНД-П». – М.: Научно-технический портал МВД России. 2017. № 1 (21). С. 17–22.
7. Тимофеев В.В. Специальная техника ОВД: металлоискатели и их использование: учеб. пособие. Барнаульский юридический институт МВД РФ. – Барнаул: АлтГТУ. – 2021. – 56 с.

Трошков Александр Михайлович,
Ставропольский государственный аграрный университет

Малофей Александр Олегович,
yzorsv@gmail.com
Ставропольский филиал
Краснодарского университета МВД России

ПРОЕКТИРОВАНИЕ ЦИФРОВОЙ ПЕРВИЧНОЙ ИДЕНТИФИКАЦИИ ПРИ ДОСМОТРЕ ЛИЧНОСТИ

Антропометрия и биометрия личности в области досмотра личности в системе МВД основывается на строении особенностей человеческого организма. За основу антропометрии и биометрии человеческого организма берется человеческий скелет. Человеческий скелет состоит из множества маленьких и крупных костей, соединенных между собой. Цифровизация идентификации личности по антропометрии основывается на общей форме и назначении. Классификация скелета человека основывается на том, что он совершенно естественно состоит из трех составляющих, рис. 1.

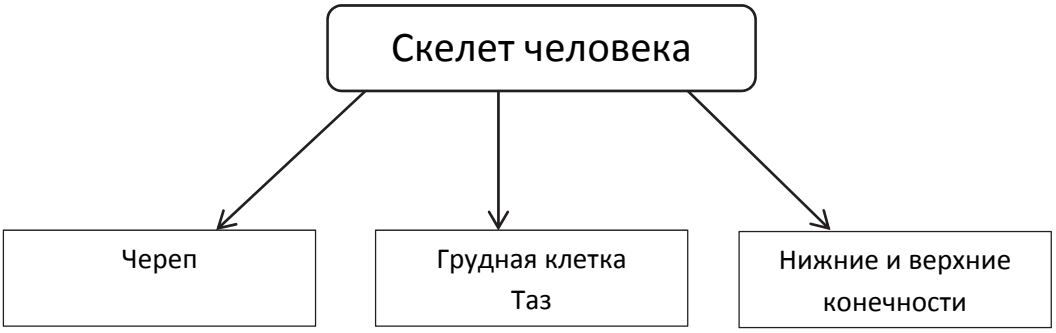


Рис. 1. Три составляющие скелета человека

С точки зрения аутентификации/идентификации антропометрию личности предлагается рассматривать в плоскостном и объемном виде, рис. 2.

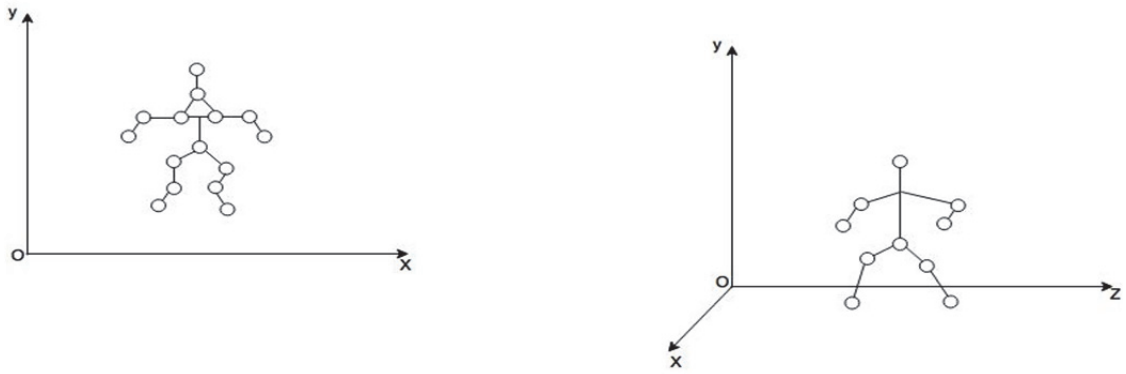


Рис. 2. Модель антропометрии в плоскостном и объемном виде

Проектируемую математическую модель антропометрии личности предлагается рассматривать в виде математической матричной системы, причем в плоскостном проекте в чистом отображении, а в объемном виде предлагается проектировать с помощью векторов, рис. 3.

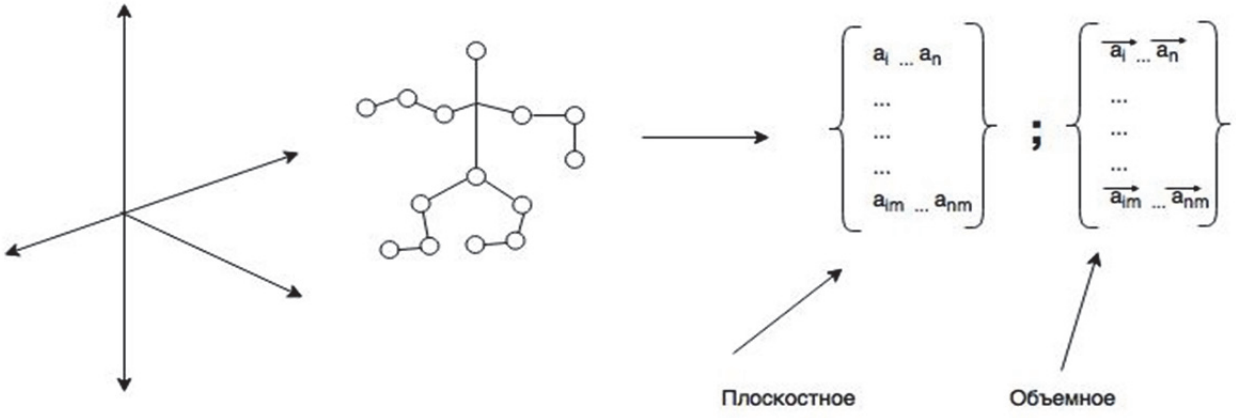


Рис. 3. Математическая модель антропометрии человека

Представленный скелет человека имеет возможность изменяться в точках соединения костей (которые представлены на рисунке 3), исходя из этого, человеческий скелет может приобретать различные позы, а с точки зрения математики фигуры, как известно соединения точек линий выражает человеческую фигуру. Для первоначальной обработки антропометрической информации можно рассмотреть три основных позиции, таблица 1.

Таблица 1

Основные позиции

Название / № позы	1. Позиция стоя	2. Позиция сидя	3. Позиция лежа
1–3			
1–3			
1–3 Матрица an			

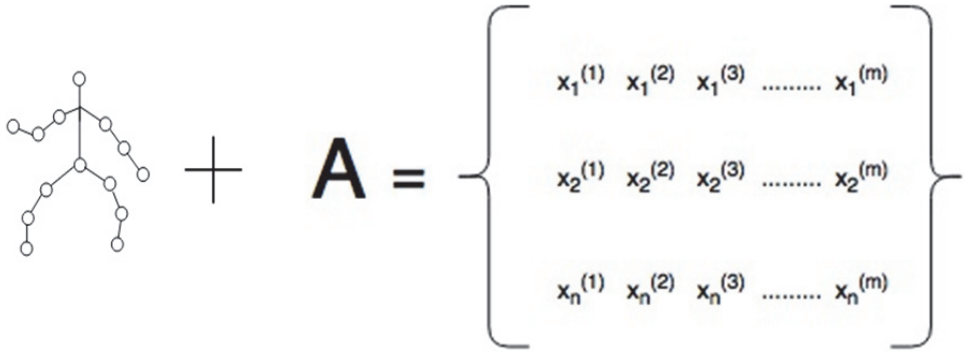
Исходя из основных позиций антропометрической информации плоскостная математическая, обработка осуществляется построением матрицы m x n, которая накладывается на выбранную позицию человеческого скелета, рис. 4.

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

1	2	3	4	5	6	7	8	9	10
2	0	0	0	1	1	0	0	0	0
3	0	0	0	1	1	0	0	0	0
4	0	1	1	1	1	1	0	0	0
5	0	1	1	0	0	1	0	0	0
6	0	0	0	1	1	1	1	0	0
7	0	0	1	0	0	1	0	0	0
8	0	1	1	0	0	1	0	0	0
9	0	1	1	0	0	1	0	0	0
10	0	0	0	0	0	0	0	0	0

Рис. 4. Проектирование матрицы антропометрии человека

Объемная математическая обработка предлагается с помощью операций с векторам $\overrightarrow{a_n}$ ….. $\overrightarrow{a_m}$. (1)



Таким образом, формировать расчеты параметров определения антропометрической характеристики, расположенной в пространстве предлагается по математическим операциям с матрицами.

Проектирование цифровой системы начинается с получением цифрового информационного кода на вход устройства обработки информации [2] (рис. 5), которое обработанный сигнал отправляет в ОЗУ. ОЗУ – работает совместно с устройством коррекции и устройством сравнения по мнемофигурезаложенной в ЦИК. Устройство принятия решения осуществляет действие через исполнительное устройство и осуществляет управление доступом [3, 4].

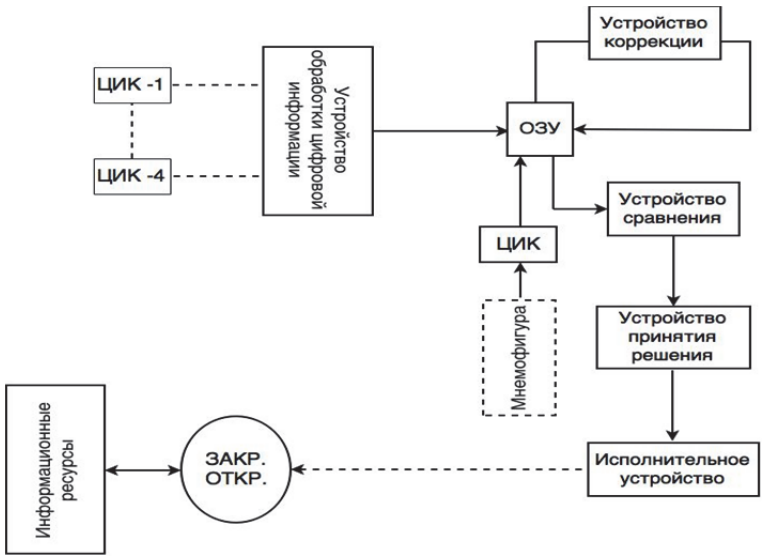


Рис. 5. Система идентификации человека по мнемознакам скелета и доступом к информационным ресурсам

На основании проекта система идентификации человека по мнемознакам и доступом к информационным ресурсам разработан алгоритм синтеза информационного кода, рис. 6.

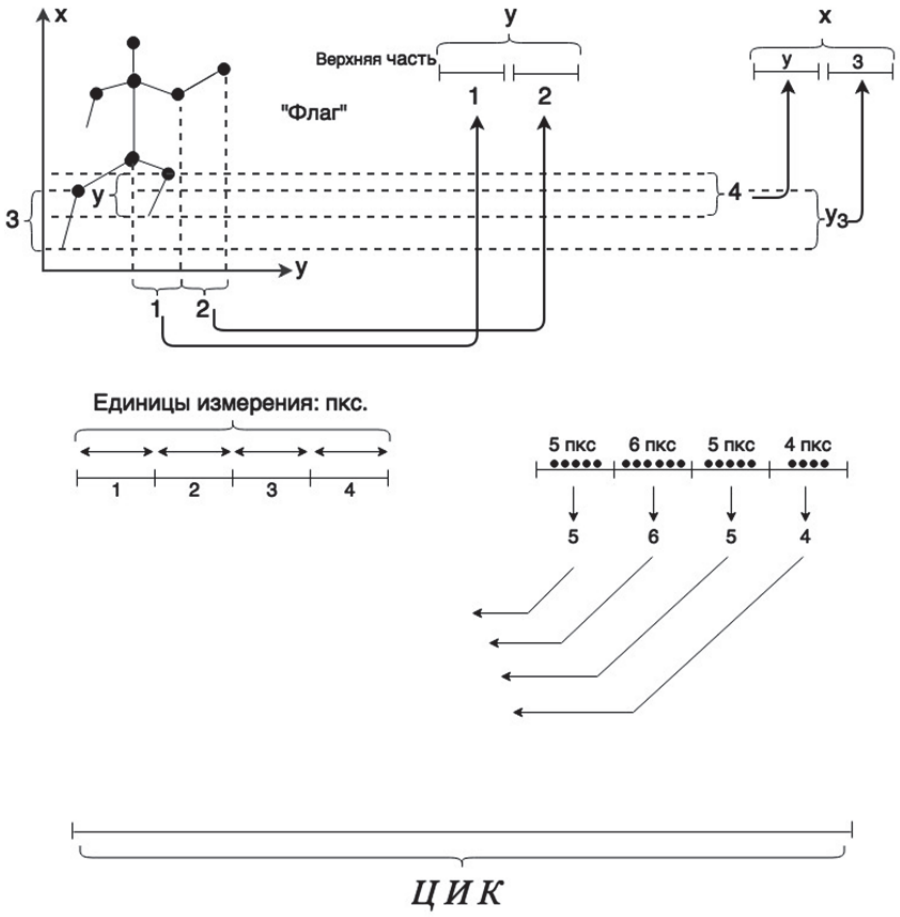


Рис. 6. Алгоритм синтеза расширенного информационного кода
по мнемоантропометрии отличительных параметров скелета человека

Идентификация личности по мнемоантропометрии отличительных параметров повышает качество определения личностных показателей. На основе выше изложенного разработан алгоритм идентификации по мнемознакам скелета и структурная схема, рис. 7.

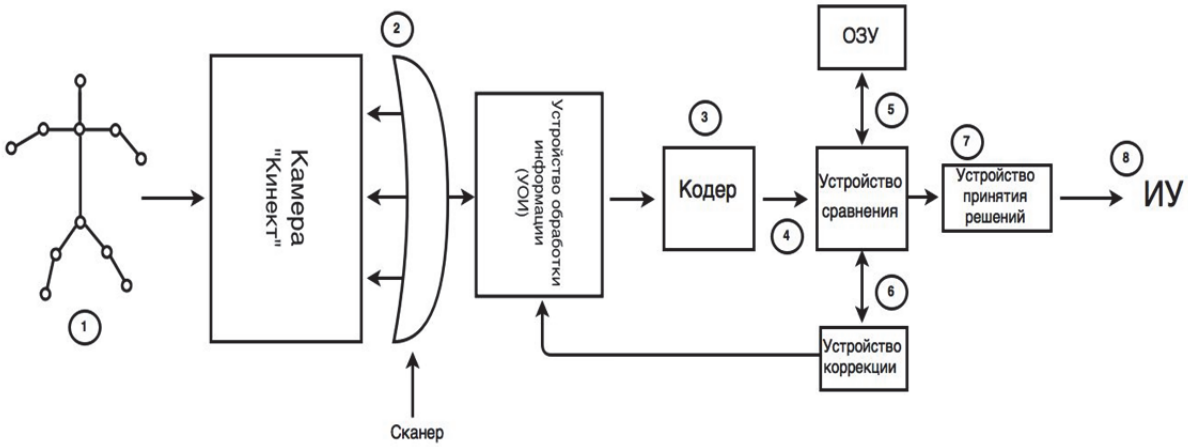


Рис. 7. Алгоритмизация и структурная схема идентификации скелета
по антропометрическим мнемознакам

В настоящее время в связи с угрозой террористического воздействия на объекты с повышенной безопасностью, уделяется большое внимание работе сотрудников специальных служб. В целях повышения качества селекции подозрительных личностей предлагается проект алгоритма первичной идентификации по антропометрическим значениям мнемознаковой структуры [1]. Этот алгоритм, представлен на рис. 8.

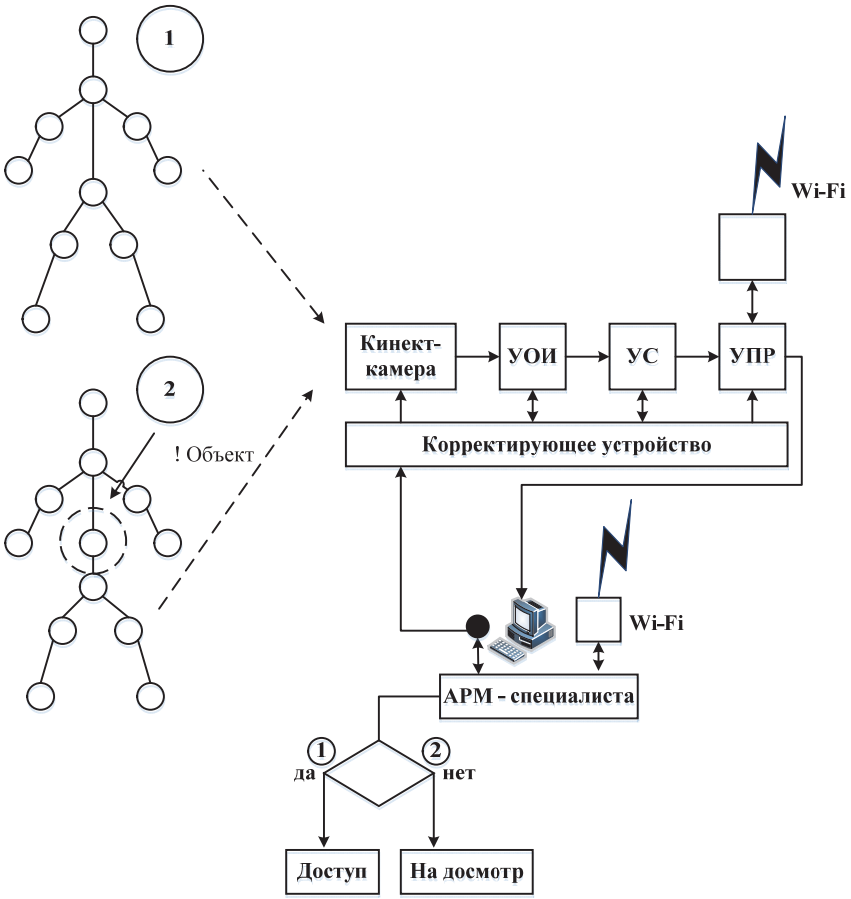


Рис. 8. Алгоритм действия первичной идентификации досмотра

Таким образом проектируемый алгоритм позволяет специальным сотрудникам служб безопасности МВД России на первичной идентификации определить подозрительных личностей по мнемоантропометрическим значениям, что существенно повысит качество досмотра и доступа к ограниченным или с повышенной безопасностью объекта.

Литература

1. Бутов Ю.И., Лепешкин О.М., Малофей А.О., Малофей О.П., Родионов В.В. Устройство имитозащиты для контролируемых объектов. Патент на изобретение RU 2439707 C1, 10.01.2012. Заявка № 2010120544/08 от 21.05.2010.

2. Трошков А.М., Трошков М.А. Информационная система аутентификации личности по биометрическим характеристикам. Свидетельство о государственной регистрации № 2012617031 6 августа 2012 года.

3. Турчина К.Е., Малофей О.П., Малофей А.О. Сравнительный анализ алгоритмов коррекции ошибок в сложных инфотелекоммуникационных системах. В сборнике: Современные технологии в нефтегазовом деле – 2020. Сборник трудов международной научно-технической конференции. 2020. С. 598–601.

4. Червяков Н.И., Бабенко М.Г., Малофей А.О., Кияшко Е.С., Стрекозова С.Ю. Разработка нейросетевой концепции активной безопасности на эллиптических кривых. Охрана, безопасность, связь. 2017. № 1-3. С. 114–124.

Челпанова Марина Михайловна,
bas-marina@yandex.ru
Крымский филиал
Краснодарского университета МВД России

ОСНОВНЫЕ УГРОЗЫ И ЭТАПЫ ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

Конец XX – начало XXI века можно признать этапом повсеместной глобализации. Однако последствия этого процесса не всегда позитивные. Международный терроризм представляет собой явление трансграничной преступности. Террористическая деятельность характеризуется наличием международных и региональных руководящих органов. Это обстоятельство необходимо учитывать правоохранительным и правоприменительным органам в целях эффективной борьбы с преступной деятельностью.

В современных условиях при борьбе с терроризмом важным является выявление источников его финансирования и их пресечение.

К источникам финансирования терроризма относят:

- денежные средства людей с террористической идеологией;
- благотворительность;
- средства от торговли наркотиками, контрабанды;
- аккумулирование и перераспределение ресурсов с использованием специально разработанных финансовых схем;
- использование международной системы «хавала» для свободного перемещения денег, драгоценных камней и металлов без сопроводительных документов;
- курьерская доставка и др.

Так, например, Росфинмониторинг фиксирует факты финансирования терроризма в России с использованием криптовалют. Чаще всего в преступных целях в России используются криптовалюты Bitcoin, Ethereum и Monero.

В феврале директор Росфинмониторинга Юрий Чиханчин на встрече с президентом России Владимиром Путиным сообщил, что в России разработан цифровой сервис, позволяющий анализировать криптотрансакции для выявления преступлений. Механизм называется «Прозрачный блокчейн». Планируется, что он позволит ведомствам «увидеть все движения с криптовалютой, то есть попытки «спрятаться» за криптовалюту».

Данные источники не являются единственными, т. к. в условиях постоянного противостояния террористы разрабатывают и применяют на практике все более совершенные способы привлечения и перемещения денег. Например, в современной цифровой практике распространился такой инструмент, как криптовалюты (виртуальные валюты, денежные суррогаты).

В криптовалютах все сделки в целом абсолютно прозрачны и доступны как регулятору, так и каждому участнику системы, отсутствие эмиссионного центра и анонимность этой технологии ставят под сомнение возможность контроля операций с их использованием, а также возможность замораживания (блокирования) средств в случае финансирования терроризма. В этой связи нужно ужесточить условия использования криптовалют и включить эти технологии в правовое поле.

По этой причине в России сегодня ведется активная политика по противодействию финансированию террористической деятельности.

Реализация этой концепции направлена на достижение нескольких целей.

– соответствие международным стандартам в области ПОД/ФТ;

– оптимальная институциональная структура и достаточные ресурсы и правовая поддержка.

Достижение целей и задач данной Концепции позволит разработать эффективные методы и меры ПОД/ФТ, направленные в первую очередь на предотвращение реализации угроз национальной безопасности и рисков совершения операций (сделок), не создавая искусственных регуляторных барьеров для развития и модернизации экономики.

Борьба с финансированием террористической деятельности должна вестись государственными и специальными органами, деятельность которых должна быть направлена на своевременное обнаружение финансовых потоков с признаками террористической адресности, что, безусловно, возможно только при качественном финансовом анализе.

К борьбе с терроризмом и его финансированием крайне важно подходить комплексно. Кредитно-финансовым учреждениям целесообразно

иметь постоянно модернизированный комплекс средств, необходимых для эффективной борьбы с финансированием терроризма, включая информацию о признаках деятельности, связанной с финансированием терроризма, о возможных рисках с их разбиением на уровни и подуровни, о лицах, представляющих опасность, и иную информацию, которая может быть использована для обнаружения случаев финансирования терроризма.

К тому же важным аспектом является предоставление возможности использования такого рода информации при выявлении существующих схем по отмыванию денег с целью финансирования терроризма, а также разработке антитеррористических моделей и процедур по обнаружению таковых финансовых потоков, совершенствованию технологий их предупреждения.

Для России противодействие терроризму является одним из главнейших направлений политики начиная с 1990-х годов. Правительство, военные и правоохранительные органы ведут упорную и мужественную борьбу как с внутрироссийскими, так и с международными террористическими бандами и организациями. Одной из важнейших составляющих обеспечения пагубной деятельности террористов является ее финансирование. Без перманентного получения денежных средств террористам невозможно было бы содержать членов преступных групп, закупать для них продовольствие, обмундирование, снабжать их оружием, взрывчаткой и т. д.

Именно поэтому борьба с финансированием терроризма является наиболее эффективным способом борьбы с ним в самом начале преступного процесса. Прежде всего необходимо указать на мотивацию принятия изменений в ст. 205.1 УК РФ.

Председатель Комитета Совета Федерации по конституционному законодательству и государственному строительству А. Клишас заявил, что «одной из целей данных изменений является формирование негативного общественного отношения к любым действиям по подготовке терактов, которая является не менее опасным деянием, чем сам теракт».

Между тем данная точка зрения подвергается критике со стороны некоторых представителей юридического сообщества. Так, продолжающаяся последние годы тенденция к ужесточению М. Трепашкин, говоря о большей пользе предотвращения преступлений, чем усиления суровости кары, видит эффективный путь борьбы с терроризмом не в ужесточении наказаний, а в разработке мер борьбы «на основе исследований социальноэкономических, политических, криминальных причин, истоков терроризма». Схожей точки зрения придерживается адвокат С. Бадамшин, который считает, что «борьба с терроризмом, которой, конечно, должно заниматься государство, складывается из двух вещей: борьбы и противодействия, и одно без другого не работает.

Анализируя приведенные точки зрения, можно сделать вывод, что вопрос о том, какими должны быть тактика и стратегия борьбы с терроризмом, заслуживает крайне скрупулезной проработки. В условиях различия мнений представляется необходимым перед непосредственным изменением законодательства проводить широкую научную и профессиональную дискуссию, рассматривать перспективу действия нормы права многоаспектно.

В этом смысле преждевременное изменение нормативной базы, осуществленное без тщательного анализа перспектив действенности и полезности, новых правил, будет носить волюнтаристский характер и непродуманность. Между тем уголовное законодательство должно быть наиболее тщательно выверено и проработано, ведь от качества его норм и конструкций в наибольшей степени зависит соблюдение прав и свобод человека и гражданина.

Терроризм следует рассматривать как в узком смысле – исходя из национального законодательства стран, так и в широком – как трансграничное преступление. Говоря о терроризме как о транснациональном преступлении, следует выделить основную цель преступников, а именно влияние на наднациональные отношения, посягательство на основы международного права.

С террористической угрозой необходимо бороться не только в рамках национальной системы, но и путем взаимодействия правоохранительных и правоприменительных органов государств, путем взаимодействия государств и международных организаций. Совершенствование международных стандартов по пресечению финансирования терроризма должно быть своевременным

Литература

1. Амельчаков О.И. Противодействие финансированию терроризма как направление международного взаимодействия государств. Текст: непосредственный // Проблемы правоохранительной деятельности – 2016. – № 2. – С. 131–135.

2. Голос Ислама.ru: информ.-аналит. портал. URL: https:// golosislama.com/news.php?id=21526 (дата обращения: 19.11.2019).

3. Косарев М.Н. Вопросы противодействия финансированию терроризма. – Текст: непосредственный // Вестник Уральского юридического института МВД России. – 2017. – № 1. – С. 33–36.

4. Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма от 30.05.2018 г. – Текст: электронный // Официальный сайт Президента России: [сайт] – URL: http://kremlin.ru/ supplement/5310 (дата обращения: 02.06.2020).

5. Пояснительная записка к проекту федерального закона «О внесении изменений в статью 205.1 УК РФ» // Система обеспечения законодательной деятельности: сайт. URL: https://sozd.duma.gov.ru/bill/230595–7 (дата обращения: 19.11.2019).

6. Росфинмониторинг: терроризм финансируют с помощью криптовалют https://www.kommersant.ru/doc/4742059

7. Совфед одобрил закон о пожизненном заключении за вербовку в террористы // ТАСС: сайт. URL: https://tass.ru/politika/4843463 (дата обращения: 19.11.2019).

Шишина Елена Александровна,
etolena8483@mail.ru
Крымский филиал
Краснодарского университета МВД России

Дячко Николай Андреевич,
dyachko99@mail.ru
Крымский филиал
Краснодарского университета МВД России

СЕТЕВЫЕ УГРОЗЫ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ И ПЕРСПЕКТИВЫ

На пороге XXI века мир вновь вернулся к противостоянию государств. Однако сегодня на международной арене нет места традиционным войнам, в виду того, что исторический опыт, раз за разом, свидетельствует о значительных потерях, измеряемых не только количеством человеческих жертв, но и крахом экономической и политической систем. Противостояние переросло в формат гибридных войн, информационных войн, информационного оружия, психологических войн и т. д.

Подмена понятий, замена ценностей, применение механизмов воздействия на психику преследует цель дальнейшего внедрения желаемых поведенческих шаблонов. Механизм воздействия на психику индивида, как правило, происходит через использование способности добиваться желаемых результатов на основе добровольного участия, предпочтений, симпатии и привлекательности для индивида. Как следствие, подконтрольность поведения индивида, в свою очередь, позволяет 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.

Среди названных проблем особого внимания ученых и правоприменителей заслуживает экстремизм. Сегодня научное сообщество прогнозирует тенденции развития экстремизма, среди которых:

а) повышение уровня организованности экстремистских групп, в условиях их самоорганизации благодаря наличию соответствующих социальных сетей;

б) слияние экстремистских объединений с организованными преступными группировками транснационального, общеуголовного и экономического характера;

в) создание устойчивых групп с экстремистской идеологией, имеющих такую же установку на действия;

г) глобализационные процессы экстремизма;

д) большое распространение экстремистских убеждений, идеологий в Интернет пространстве и т. д.

Безусловно, 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**.** Концепция общественной безопасности Российской Федерации, как стратегический документ среди современных угроз определяет использование Интернета экстремистскими организациями для рассылки экстремистских материалов, привлечения в свои ряды новых членов и координации преступной деятельности организации. Вырастает число веб-сайтов, количество людей, которые видят в Интернете самый легкодоступный метод для прямых призывов к экстремизму. Так к примеру, более 300 000 акантов в «Twitter» согласны с идеологией ИГ-ДАИШ, либо интересуются данной идеологией. В день на один из аккаунтов в «Twitter» данной организации может подписать от 2 до 70 тыс. человек, которые могут быть неумышленно вовлечены в распространение экстремистско-террористических взглядов и новостных фейков про данную организацию.

В целях зашиты национальной безопасности государства, здоровья, прав и законных интересов граждан, целесообразно противопоставить пропагандисткой экстремистской экспансии адекватные меры противодействия. Не смотря на значимость и актуальность противодействия экстремизму, в представленном направлении работы все же имеется ряд проблемных вопросов.

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.

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 все, 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.

Опыт других стран подтверждает тот факт, что использование мер, касающихся ограничения доступа к определенным интернет-ресурсам, в том числе и другие методы информационной изоляции и подавления, имеют достаточно ограниченную эффективность в борьбе с использованием сети Интернет в деятельности террористических и экстремистских организаций и могут быть успешно преодолены.

Проблема противодействия в сети Интернет состоит в том, что большой информационный массив, накапливаемый в Интернете представлен в виде текстов, графических изображений (рисунки, фото, видеоизображения), что представляет сложность идентификации материалов как экстремистских. Не простым является и идентификация материалов со списком экстремистских материалов.

Одним из способов обнаружения признаков подготовки к преступлению является мониторинг информационного пространства. С целью информационного противодействия экстремизму ведомственными приказами созданы отдельные подразделения на базе подразделений по противодействию экстремизму. К их функциям отнесен мониторинг сети Интернет пространства с целью: установления интернет сайтов радикального характера; поиска сведений о противоправных действиях экстремистской направленности; поиска информации о возможных местах совершения противоправных акций и т. д. Мониторинг Интернет–пространства дает возможность оперативно добыть значительный объем информации о действующих экстремистских группах, местах встреч, распределении ролей в экстремистской группе, а также сведения об их руководителях, организаторах и исполнителях.

Совершенствованием данного направления деятельности является автоматизированный поиск и анализ информации, которая по формальным признакам образует даяния экстремистской направленности. Такие зарубежные страны как Китай, Корея уже давно применяют так называемые програмы-роботы, которые осуществляют мониторинг интернет сайтов.

В правоохранительных органах Российской Федерации также внедрены программные комплексы для автоматического выявления пользователей социальных сетей, вовлеченных в социально опасные процессы и явления (распространение экстремистских материалов, идеологии терроризма, призывов к насилию, распространяющих наркотические вещества, вовлеченных в незаконный оборот оружия и изготовление СВУ, оккультные течения, АУЕ, суицидальные группы, School Shooting, «Колумбайн» и т. д.). Сбор, обработка, структурирование больших пользовательских данных, систематический анализ пользовательских медиа на предмет наличия информации деструктивного характера, выявление пользователей, вовлеченных в социально опасные явления и процессы с последующей их идентификацией позволит анализировать и оперативно реагировать на складывающуюся оперативную обстановку. Данный подход эффективен, как при осуществлении превентивных мер, так и при пресечении преступных деяний.

Интерес представляет и зарубежный опыт применения полицейской разведки с целью оперативно-розыскного прогнозирования. В основе указанного метода лежит получение упреждающей информации и составление на основании этой информации мысленной модели вероятного развития какой-либо ситуации, то есть предположения о том, как будет развиваться оперативная обстановка. Систематизируется информация о вероятном поведение лиц, представляющих оперативный, предположительном развитии ситуации в период документирования их преступной деятельности, прогнозирование эффективного использования сил и средств оперативно-розыскной деятельности.

При борьбе с преступными проявлениями экстремистской направленности в сети Интернет особое значение имеют оперативно-розыскные мероприятия (далее – ОРМ), которые являются неотъемлемым элементом в алгоритме доказывания по уголовным делам данной категории. Одним из наиболее результативных ОРМ в данной сфере является «оперативное внедрение» в сети Интернет. Криминалистически значимая информация, полученная сотрудниками оперативных подразделений при его осуществлении, может быть, как оперативной, так и доказательственной. Информация, полученная посредством сети Интернет, в том числе из социальных сетей («ВКонтакте», «Одноклассники», «Facebook» и т. п.) изначально является оперативной (ориентирующей). Впоследствии, при соблюдении определенных условий, она может стать доказательственной. Согласно данным исследования, проведенного И.В. Погодиным, для преступлений, предусмотренных статьями 282, 282.1, 282.2 Уголовного Кодекса Российской Федерации в 30% случаев оперативная информация становится основанием проведения доследственной проверки при возбуждении уголовного дела, примерно в

50% случаев – трансформируется в доказательства и в последующем является основой обвинения, а в остальных случаях – позволяет оптимизировать направление расследования.

Любая информация, подлежит проверке. В ходе проверки устанавливаются фактические данные, содержащие признаки экстремистских действий. Принимая во внимание, что сведения, содержащиеся в Интернете, могут быть удалены в любой момент, сотрудники ОВД должны зафиксировать факт размещения конкретного видеофайла в ресурсе, о чем составить протокол осмотра страницы пользователя. При осмотре страницы пользователя необходимо не только установить точный адрес интернет-странички с видеофайлом, наименование видеоматериала и длительность, но и дату выпуска, а также пользователя, разместившего видеофайлы. В конце необходимо записать полученные сведения на носитель (CD, DVD) который должен содержать его характеристику, в том числе серийный номер. Осуществление этих действий гарантирует отслеживание копий экстремистских материалов, размещенных в Интернете, и возможность проверки подлинности цифровых доказательств.

Значительные проблемы сохраняются и при проведении лингвистической экспертизы материалов экстремистского характер по причине отсутствия единой методики проведения лингвистической экспертизы, а также большой загруженности специалистов и экспертов.

Таким образом, информационное противодействие экстремизму в настоящее время является приоритетным направлением. Ввиду большого объема информации содержащейся в Интернет пространстве, требующей постоянного мониторинга, меры по выявлению и блокированию экстремистского контента целесообразно в большей степени переложить на автоматизированные системы мониторинга. Успех противодействия экстремизму лежит в комплексном подходе, представляющим собой совокупность методов: метод административного влияния на провайдеров, владельцев вебсайтов и блогов; технический – по выявлению информации экстремистского содержания; оперативно – розыскной метод направленный на выявления и пресечение деятельности лиц, размещающих материалы экстремистского характера в сети Интернет.

Литература

1. Затолокин А.А. Противодействие экстремизму в деятельности подразделений полиции: учеб.-практ. пособие. – Краснодар: Краснодарский университет МВД России, 2018.

2. Лапунова Ю.А., Голяндин Н.П. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их

решения / Труды академии управления МВД России Учредители: Академия управления МВД России (Москва), 2017.

3. Куликов Е.М., Кубякин Е.О., Корников Д.И. Информационный экстремизм в современном российском обществе [Текст]: учебное пособие; Краснодарский ун-т МВД России. – Краснодар: Краснодарский ун-т МВД России, 2016.

4. Миронова С.Н. и др. Противодействие органов внутренних дел экстремизму и терроризму: учеб. пособие / под ред. Ф.К. Зиннурова. – М.: 2018.

5. Погодин И.В. Доказывание по делам о преступлениях экстремистской направленности: автореферат дис. ... канд. юрид. наук: 12.00.09 / Погодин Илья Владимирович, Москва, 2012.

6. Шишина Е.А. Информационные угрозы, как угроза национальной безопасности Российской федерации: постановка проблемы/ Правовые средства обеспечения национальной безопасности Российской Федерации: история и современность: материалы междунар. науч.-практ. конф., Иркутск, 24 апр. 2020 г. / отв. ред. Е.М. Якимова. − Иркутск: БГУ, 2020.

7. Шамаев Г.П., Подкатилина М.Л. О фиксации видеоматериалов экстремистской направленности, размещенных в сети интернет // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА); Известия Тульского государственного университета. Экономические и юридические науки, 2013.

8. Щербакова Л.М. Некоторые проблемы борьбы с экстремизмом и терроризмом в современных условиях // Общество и право (4), 2014.

Научное издание

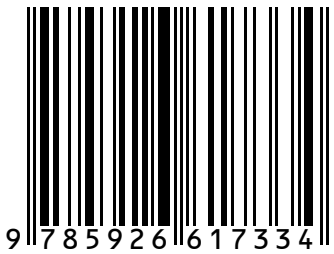
ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции

(23 апреля 2021 г.)

В авторской редакции
Компьютерная верстка *С. В. Коноваловой*

ISBN 978-5-9266-1733-4



Подписано в печать 02.08.2021.
Авт. л. 8,0. Заказ 151.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.