Краснодарский университет МВД России

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции
(24 мая 2024 г.)

Краснодар
2024

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. (24 мая 2024 г.) / редкол.: А. В. Еськов, В. И. Еремченко, А. К. Назаров и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2024. – 1 электрон. опт. диск.

ISBN 978-5-9266-2038-9

В сборнике представлены материалы Всероссийской научно-практической конференции «Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму», состоявшейся в Краснодарском университете МВД России 24 мая 2024 г.

Для профессорско-преподавательского состава, 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 978-5-9266-2038-9

Оглавление

Васильева Татьяна Борисовна,
старший преподаватель кафедры
информационно-правовых дисциплин
и специальной техники
Сибирского юридического института МВД России

Казарина Юлия Николаевна,
слушатель Сибирского юридического института МВД России

ИСПОЛЬЗОВАНИЕ ПРОГРАММ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

На сегодняшний день достаточно широко распространено использование искусственного интеллекта для решения задач различной сложности. Одним из самых перспективных направлений искусственного интеллекта являются нейронные сети. Уникальность нейросетей заключается преимущественно в том, что они работают наподобие человеческого мозга. Они состоят из множества соединенных между собой различных нейронов, которые образуют организованные слои. Суть работы нейронов заключается в том, что каждый нейрон получает входящую информацию, затем ее обрабатывает и передает последующему нейрону, входящему в организованный слой. Данный процесс передачи информации происходит с помощью весов, которые настраиваются в процессе обучения сети. Нейронные сети способны обучаться на данных, выявлять закономерности и паттерны в информации, делать прогнозы и принимать решения на основе полученных знаний.

На основе методов искусственного интеллекта создаются и развиваются различные программные системы, сущность которых направлена на решение задач различной сложности таким образом, как это делал бы человеческий мозг. К наиболее популярным направлениям применения нейросетей относятся прогнозирование различных ситуаций, оценка любой цифровой информации, включая неструктурированные данные, с попыткой дать по ней заключение, а также анализ информации с поиском скрытых закономерностей.

Отметим, что использование программ искусственного интеллекта не обошло стороной и правоохранительные органы. Современное общество развивается стремительно и правоохранительной системе следует не отставать от этих технологий в целях своевременного реагирования, реализации и предупреждения преступных деяний. Применение современных технологий способствует значительному повышению эффективности и оперативности их работы, помогает выявлять преступления, идентифицировать преступников и предотвращать преступления.

Искусственный интеллект может быть использован для анализа крупных объемов данных, выявления и прогнозирования преступной деятельно-

сти, обеспечения безопасности общества. Аналитические инструменты могут помочь в выявлении закономерностей, моделировании преступных схем, анализе видеозаписей для идентификации преступников.

Наиболее популярными нейросетями, применяемыми в правоохранительных органах являются такие программы, функционирование которых заключается в работе с визуальным контентом, а именно со сканированием, распознаванием, анализом и прогнозированием.

Так, нейросети используются для распознавания лиц на видеозаписях или фотографиях, что помогает в установлении личности человека, а также его местонахождении. Также нейросети могут использоваться для определения местоположения человека на основе данных GPS или сети мобильной связи.

Обработка графической информации вручную может привести к ошибкам из-за усталости и других факторов. Машины, оборудованные специальным программным обеспечением компьютерного анализа, способны обрабатывать изображения достаточно точно. Программы искусственного интеллекта способны оценивать изображение. На основе анализа индивидуальных характеристик лица человека они способны отличать одно человеческое лицо от другого. Использование таких систем позволяет автоматизировать процессы распознавания и анализа графической информации, что улучшает эффективность и точность работы.

Тем не менее, нейросеть может выявлять похожие лица и таким образом вводить в заблуждение сотрудников правоохранительных органов. Например, в 2023 году в аэропорту г. Ярославля по ошибке нейросети был задержан ученый. Он оказался похож на преступника, на которого составили фоторобот. Нейросеть определила, что схожесть составляет 55% . Именно поэтому ученые и практики выполняют дополнительную экспертную идентификацию с использованием различных методов и методик, включающих дактилоскопию, личную беседу и прочее.

Правоохранительными органами применяется целый ряд многообразных информационно-поисковых систем, функционально предназначенных для раскрытия и расследования преступлений:

1. Система «Блок» способствует информационному обеспечению расследования преступлений в сфере экономики.
2. Система «Маньяк» обеспечивает получение информации при расследовании серийных убийств.
3. Система «Спрут» помогает в установлении контактов и соответствующих связей среди преступников.
4. Система «Сейф» содержит в себе информацию о хищении денежных средств из хранилищ.
5. Система «Зеркало» содержит в себе различные географические, фактографические и статистические сведения.

Несмотря на все вышеперечисленные преимущества нейросети, не стоит забывать и об опасности, которая таится в самом ее функционировании и возможностях. Любые технологии могут использоваться и развиваться

не только во благо, но и в корыстных целях. Так, люди могут использовать возможности нейросети в целях нарушения приватности какой-либо информации, злоупотребления полученных сведений, в целях совершения преступных действий. Также к негативным проявлениям можно отнести недоверие, предвзятость, искажение данных и качества полученной информации со стороны самих сотрудников правоохранительной системы. Еще одним из самых главных минусов нейросети является замещение человеческого труда: внедрение автоматизированных систем, основанных на нейросетях, может привести к потере рабочих мест и усилению социальных неравенств.

Таким образом, актуальность и повсеместная востребованность развития и изучения программ искусственного интеллекта в современном обществе трудно переоценить. Нейронные сети стали одним из значимых инструментов в области программ искусственного интеллекта, и их популярность продолжает расти. Новые исследования и разработки в этой области постоянно совершенствуют работу нейросетей, что позволяет им решать все более сложные задачи. Нейронные сети будущего, скорее всего, будут способны работать с еще большими объемами данных и анализировать их более быстро и точно, что откроет новые возможности для их применения.

Инструменты современных технологий применяются не только в благоприятном направлении для общества, но и направлены на совершение преступных деяний. Причем данная преступная деятельность переходит в цифровое пространство и осуществляется с использованием программ искусственного интеллекта, так как это позволяет остаться личности преступника анонимной, что, в свою очередь, способствует повышению числа нераскрытых преступлений и безнаказанности преступников.

Высокая степень развития, популярность и доступность информационных технологий требует совершенствования инструментов, средств и методов, способствующих своевременному раскрытию, улучшению качества работы и профессионального уровня правоохранительных органов. Данные меры позволят правоохранительным органам идти в ногу со временем, а также занимать лидирующие позиции в борьбе против цифровой преступности.

Литература

1. Безгачев, Ф. В. Применение искусственного интеллекта (нейронных сетей) в деятельности полиции / Ф. В. Безгачев // Закон и власть. – 2023. – № 3. – С. 78-82. – EDN GCAYHA.

2. Гордеев, А. Ю. Перспективы развития и использования искусственного интеллекта и нейросетей для противодействия преступности в России (на основе зарубежного опыта) / А. Ю. Гордеев // Научный портал МВД России. – 2021. – № 1(53). – С. 123-135. – EDN KNBLSY.

3. Информационное агентство ТАСС : официальный сайт . – URL: https://tass.ru (дата обращения: 19.04.2024). – Текст : электронный.

4. Качагина, К. С. Нейронные сети - перспективы развития / К. С. Качагина, А. Д. Сафарова // E-Scio. – 2021. – № 2(53). – С. 34-39. – EDN WVYKGJ.

Васильева Татьяна Борисовна,
старший преподаватель кафедры
информационно-правовых дисциплин
и специальной техники
Сибирского юридического института МВД России

Кузнецова Ольга Владимировна,
слушатель Сибирского юридического института МВД России

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ И РАСКРЫТИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ

В настоящее время значительно возрастает количество преступлений, совершенных путем дистанционного мошенничества. Настоящий научный обзор посвящен особенностям раскрытия и расследования преступлений, совершенных путем применения информационно-телекоммуникационных технологий (ИТТ).

Данная тема является актуальной, поскольку в настоящее время происходит рост преступлений, связанных с дистанционным мошенничеством. Причем виды данных преступлений различны, а тактика работы преступников периодически меняется, усовершенствуется, и появляются новые виды дистанционных мошенничеств. При этом преступные схемы дистанционных мошенничеств, придуманные преступниками ранее, также продолжают использоваться. Однако раскрыть данные преступления нелегко, а зачастую просто невозможно.

«Любые инновации в интернет-пространстве создают предпосылки для расширения сферы ее криминализации. Возникли сложности и у представителей правоохранительных структур в расследовании таких дел, так как анонимность глобального пространства позволяет виртуальному преступнику не оставлять следов преступления, в результате чего его обнаружение и нейтрализация практически невозможны.»

В.И. Лустин под дистанционным мошенничеством понимает «вид мошенничества, осуществляемого преступником дистанционно, по большей части используя телефонные либо компьютерные сети, через которые он путем обмана воздействует на потерпевшего и убеждает его передать свое имущество удаленным способом» .

Одним из видов дистанционного мошенничества является звонок на сотовый телефон потерпевшего либо на стационарный телефон и сообщение гражданину о том, что его родственник попал в дорожно-транспортное происшествие, затем сообщает информацию о том, что возбуждено уголовное дело, для прекращения которого необходимо передать денежные средств. Потерпевший, доверяя словам неустановленного лица, и действуя по его указанию, при помощи банкоматов, приложений банков и других средств

переводит свои денежные средства мошенникам либо передает денежные средства курьеру.

В данном случае следователю необходимо выяснить, с каких абонентских номеров поступали звонки. Если звонок поступал на мобильный телефон, то органами предварительного расследования запрашивается детализация с абонентского номера потерпевшего, таким образом, номера, с которых поступали звонки, устанавливаются в кратчайший срок. Путем направления соответствующих запросов следователям удается установить банк, в который были переведены денежные средства, получателя денежных средств, номер счета, номер банковской карты. Кроме того, следователь направляет ходатайство в суд о необходимости заблокировать банковский счет получателя.

Однако в случае, если звонки поступали на стационарный номер потерпевшего, установить абонентские номера, с которых осуществлялись звонки, сложнее, чем если бы они поступали с мобильного номера. В данном случае следователю необходимо направить запрос оператору связи и получить ответ, что на практике занимает довольно длительный период времени.

Еще одним из распространенных видов дистанционного мошенничества является то происшествие, когда звонки осуществляются через

интернет-мессенджеры, такие как «WhatsApp», «Telegram», «Viber» и другие. Звонки, осуществляемые через интернет-мессенджеры не отображаются в детализации абонентского номера потерпевшего и отследить номер, с которого был осуществлен звонок, становится в разы сложнее.

В настоящее время приобретает популярность такой вид мошенничества, как взлом личного кабинета на сайте «Государственных услуг». Злоумышленник, получая доступ к личному кабинету потерпевшего, получает и полный доступ к его персональным данным и личной информации о потерпевшем, что в последующем позволяет преступнику оформить на имя потерпевшего кредиты и микрозаймы.

Мошенники, осуществляя звонки потерпевшему, представляются сотрудниками оператора сотовой связи, которую использует потерпевший, и под предлогом продления договора связи просят назвать код из

смс-сообщения. Потерпевший в свою очередь сообщает код, после чего мошенники получают доступ к личному кабинету потерпевшего на сайте «Государственных услуг». Таким образом, мошенники могут получить доступ даже к банковским счетам потерпевшего.

Необходимо понимать, что проблема данной темы кроется во многих аспектах криминалистической характеристики дистанционного мошенничества. Первым аспектом является объект преступного посягательства. Вторым аспектом, имеющим пробел, является личность преступника и его характеристика. Третьим, немаловажным, аспектом выступает личность преступника. Четвертым аспектом выступает мотив совершения преступления.

Объектом преступного посягательства дистанционных преступлений являются денежные средства потерпевших.

Главная сложность в раскрытии и расследовании преступлений, связанных с дистанционным мошенничеством, является установление личности преступника, а также его местонахождение. Недостаточно установить лицо, которому принадлежит абонентский номер, следователю необходимо доказать, что именно данное лицо осуществляло звонки на абонентский номер потерпевшего и именно оно совершило данное преступление.

В практической деятельности органов предварительного следствия бывают эпизоды, когда лицо, осуществляющее звонки на абонентский номер потерпевшего, и получатель денежных средств – это два совершенно разных человека, не имеющих друг к другу никакого отношения.

Зачастую мошенники осуществляют звонки на абонентские номера потерпевших с других регионов Российской Федерации и даже из других государств. Кроме того, при звонке мошенники используют систему VPN, поэтому определить, откуда и с какого номера был осуществлен звонок, становится практически невозможно.

Становится очевидным, что при расследовании дистанционных мошенничеств возникает достаточно много проблем и сложностей. И, на самом деле, решать их очень сложно, потому что каждая ситуация индивидуальна, а законодатель не может предусмотреть все.

На наш взгляд, пробелы в законодательстве могут быть нейтрализованы только усовершенствованием процедуры рассмотрения изучаемой категории дел. Кроме того, считаем, что имеется необходимость в усовершенствовании взаимодействия операторов сотовой связи с органами предварительного расследования с целью исключения таких ситуаций, когда операторы сотовой связи предоставляют абонентские номера, не проверяя личные персональные данные абонента, предоставляют абонентские номера иностранным гражданам, не имеющим постоянного места жительства или регистрации на территории Российской Федерации.

Считаем, что проблемы, возникающие в рамках раскрытия и расследования дистанционных мошенничеств, необходимо решать комплексно, при взаимодействии со всеми правоохранительными структурами и организациями, осуществляющими взаимодействие и содействие правоохранительным органам в раскрытии и расследовании преступлений.

Литература

1. Гедугошев, Р. Р. Международное сотрудничество в правоохранительной сфере по вопросам противодействия экстремизму и терроризму / Р. Р. Гедугошев, Е. В. Кузнецова, Т. Б. Васильева // Журнал прикладных исследований. – 2021. – № 4-2. – С. 77-81. – DOI 10.47576/2712-7516_2021_4_2_77. – EDN ITFFMJ.

2. Лустин, В. И. Дистанционные мошенничества / В. И. Лустин // Закон и власть. – 2023. – № 5. – С. 67-74. – EDN MPLWGO.

3. Халитова, В. З. Проблема раскрытия дистанционных мошенничеств / В. З. Халитова, Р. Р. Галяутдинов // Международный журнал гуманитарных и естественных наук. – 2022. – № 12-5(75). – С. 117-119. – DOI 10.24412/2500-1000-2022-12-5-117-119. – EDN DSTJEW.

Власенко Александра Владимировна,
кандидат технических наук, доцент,
доцент Краснодарского университета МВД России

ИНФОРМАЦИОННЫЙ ЭКСТРЕМИЗМ И ФЕЙКОВЫЙ КОНТЕНТ КАК НОВЫЙ ВЫЗОВ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные и телекоммуникационные технологии играют ключевую роль в противодействии экстремизму и терроризму.

Эти технологии помогают правоохранительным органам и специализированным службам отслеживать подозрительные активности в сети, мониторить социальные медиа и веб-ресурсы, блокировать террористические и экстремистские материалы, а также отслеживать коммуникации между подозреваемыми.

Использование информационных и телекоммуникационных технологий также позволяет оперативно реагировать на угрозы, обмениваться информацией с другими службами и странами, а также обучать специалистов и общественность по поводу соблюдения безопасности в Интернете и выявления признаков радикализации.

Экстремизм и терроризм в сфере информационных и телекоммуникационных технологий имеет большое и негативное влияние представляют серьезную угрозу для общественной безопасности, что требует эффективных мер для предотвращения и противодействия таким опасным проявлениям в сети.

Роль социальных сетей в распространении информационного экстремизма заключается в том, что они позволяют быстро и легко распространять информацию среди широкой аудитории.

Экстремистские группы могут использовать социальные сети для создания сообществ, где они могут делиться своими идеями и привлекать новых сторонников. Они также могут использовать социальные сети для организации акций протеста или других действий.

Кроме того, социальные сети представляют возможность создавать фейковые аккаунты и распространять ложную информацию, что обычно приводит к дезинформации и манипуляции общественным мнением.

На начало 2024 года общее число активных учетных записей в социальных сетях насчитывает 5,04 млрд.

Так их количество значительно выросло, а сам рост составил 5,6% за последний года, в то время как в 2023 году в социальных сетях было зарегистрировалось 266 млн. новых пользователей.

Такая впечатляющая цифра означает, что за последний год в среднем, в мире создавалось 8,4 новых учетных записей каждую секунду..

Для борьбы с информационным экстремизмом и фейковым контентом приняты законодательные меры:

- введение уголовной ответственности за распространение фейковый новостей и дезинформации;
- усиление контроля над распространением информации в интернете, включая социальные сети;
- создание специализированных органов для борьбы с фейковыми новостями и дезинформацией;
- разработка российского программного обеспечения для автоматического выявления и блокировки фейкового контента.

В 2023 г. фиксируется рост примерно в 8 раз фейковой информации по сравнению с 2021г. Фактически сформирован устойчивый тренд на повышение доли фейков в российском сегменте с прогнозируемым стабильным ростом в 2023-2024 годах.

Фейки по своей сути являются некой новостью гиперболизированной степени из-за чего привлекает достаточно много внимания реципиента. Так фейковые новости в сравнении с обычными попадают во внимание адресата в 6 раз быстрее, означая, что вероятность ретвита у каждого фейка на 70% выше в сравнении с обычной новостью.

Фейки являются «новостью» в превосходной степени, обращая на себя больше внимания и неся больше негативных последствий.

Давайте рассмотрим маркеры фейковый новостей:

- эмоции: фактор страха/опасности;
- фактоиды и тезисы;
- указание важности или срочности Ссылка на «достоверный» источник;
- утверждение достоверности;
- геопривязка;
- призыв к распространению;
- призыв к действию или бездействию;
- лингвистические конструкции «раскрытия правды» («наконец выяснилось», «нас обманывали», «информация от друга из ФСБ/МВД» и т.п.);
- долгожданная новость, изобличающая «правду»;
- теория «заговора»;
- просьба поделиться и распространить и др.

На сегодняшний день существуют различные методы противодействия фейковым новостям, такие как: знание и применение операторов поисковых сетей; умение работать определенным образом с программным обеспечением обеспечивающим редакцию фото и видео контента («Photoshop», «SonyVegas»); использование открытых данных при помощи функционала вспомогательных программ и сервисов («Google maps», «Wolfram Alpha», «TinEye», «WayBack Machine») а так же оценка речевого тракта говорящего, который можно воссоздать средствами моделирования.

На человеческую речь влияют анатомические особенности его голосового аппарата: связок, языка, челюстей, губ.

При генерации звуков (фонем) эти участники процесса используются по разному, но всегда в пределах лимита заданного природой. Звуковые дипфейки не учитывают таких ограничений.

Дипфейки несколько лет назад распознавались легко, технология была слабо развита и требовала серьезных ресурсов для создания. К настоящему моменту в открытом доступе появляется все больше ресурсов для создания дипфейков. Решения и датасеты условно бесплатные - дипфейк можно сделать на телефоне.

Создать дипфейк стало проще и дешевле, однако инвестиции в развитие технологий детекции исчисляются миллионами.

В заключение хочется отметить, что информационные и телекоммуникационные технологии начинают занимать все более важную позицию в противодействии экстремизму и терроризму.

Они позволяют быстро обнаруживать и предотвращать угрозы, мониторить активности экстремистов и террористов, а также эффективно контролировать их пропагандистские материалы.

С использованием современных технологий легче выявлять и анализировать сети экстремистов, следить за общественными настроениями, а также отслеживать онлайн-активности и пропагандистские материалы экстремистов и террористов.

Специализированные программы и алгоритмы помогают автоматически обрабатывать и анализировать огромные объемы информации, что значительно повышает эффективность контртеррористических операций.

Однако, необходимо помнить, что использование технологий в борьбе с экстремизмом и терроризмом должно соблюдать принципы законности, защиты личных данных и соблюдения прав человека.

Литература

1. Власенко А.В. , Киселев П.С. , Склярова Е.А. / Искусственный интеллект и проблемы кибербезопасности. Технология Deepfake. Информационные технологии. «Молодой ученый», № 21 (363), май 2021. С. 81-85.

2. Социология терроризма [Электронный ресурс]: учебник – Эл. изд. - Электрон. текстовые дан. (1 файл pdf: 119 с.). - Н.Ю. Григорьев, Э.Б. Родюков. 2024. – Режим доступа: http://scipro.ru/conf/sociology_terrorism2_24.pdf.

3. Патюкова Р.В., Оломская Н.Н., Николаева Ю.Е./ Механизмы создания фейковой новости как современной технологии взаимодействия с общественностью. Вестник Волжского университета им. В.Н. Татищева, №2, Т.2, 2022. С. 237-246.

Власенко Александра Владимировна,
кандидат технических наук, доцент,
доцент кафедры информационной безопасности
Краснодарского университета МВД России

Войтенко Владислав Александрович,
курсант Краснодарского университета МВД России

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

В современном мире информационная безопасность становится одним из ключевых аспектов функционирования не только отдельных организаций, но и всего общества в целом. Вдобавок, стремительное развитие технологий, особенно в области искусственного интеллекта (ИИ), вносит существенные изменения в ландшафт информационной безопасности, создавая новые возможности, и новые угрозы.

Влияние искусственного интеллекта на информационную безопасность становится объектом активного изучения и обсуждения в научном сообществе. С одной стороны, применение ИИ в области кибербезопасности обещает улучшить эффективность обнаружения и предотвращения кибератак, а также повысить защиту конфиденциальной информации, путем исключения человеческого фактора в работе. С другой стороны, с развитием технологий ИИ возникают новые уязвимости, атаки становятся более изощренными, и возникает необходимость в адаптации средств защиты.

В первую очередь разбираю тему данной статьи следует разобраться в основных понятиях, а именно «искусственный интеллект» и «информационная безопасность».

Так например, в научной работе Э.М. Продайкова дано следующее понятие искусственного интеллекта:

Искусственный интеллект (ИИ) — это наука и технология, включающая набор средств, позволяющий компьютеру на основании накопленных знаний давать ответы на вопросы и делать на базе этого экспертные выводы, то есть получать знания которые в него не закладывались разработчиком.[1]

Таким образом можно сделать вывод, что искусственный интеллект это самообучающаяся модель схожая по своим интеллектуальным параметрам на человека, поскольку как и человек из всей полученной информации он формируют своего рода структурированную базу, на основе которой может делать собственные умозаключения.

Понятие «информационной безопасности» дано в научной статье С.Э. Мерзлякова: Под информационной безопасностью понимается система

---

[1] Э.М. Продайков «Современное состояние искусственного интеллекта» - https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-iskusstvennogo-intellekta/viewer

предусмотренных законом мер различного свойства, связанных с обеспечением состояния защищенности населения от информационных угроз.[1] То есть понятие информационной безопасности несет в себе не просто защиту самой информации от посягательств, а защиту населения от угроз исходящих от информации. С этим понятием стоит разобраться поподробнее, чтобы прояснить моменты, которые вызовут неясность. Суть информационной безопасности подразумевается в защите населения от угроз, которые в информационной среде могут вызвать серьёзные проблемы. Таковыми проблемами могут являться: кража персональных данных, вымогательство денежных средств и многое другое, что непосредственно нарушает законодательство Российской Федерации и вызывает проблемы у населения страны. Так что основываясь на вышесказанном можно сделать вывод, что информационная безопасность и ее развитие является необходимой базой для обеспечения принципа защищенности у граждан.

Но возникает логичный вопрос. Как вообще ИИ оказывает влияние на информационную безопасность? Отвечая на данный вопрос следует обратиться к научной статье блога компании Neuro.net «Как ИИ кибербезопасность усиливает: новые тренды и возможности»[2]. Основываясь на данной там информации можно выявить направления информационной безопасности в которых искусственный интеллект оказывает свое непосредственное влияние.

1. Обнаружение киберугроз. Машинное обучение, которое использует в своей основе ИИ позволяет в режиме реального времени постоянно анализировать все данные которые поступают из различных источников. Такие алгоритмы, с помощью которых работает машинное обучение, все больше и больше совершенствуются с каждым днем, что позволяет с большей эффективностью противостоять различным типам атак. Алгоритмы благодаря анализу данных и моделей поведению могут понимать все важные аспекты инфраструктуры и сети организации, а также возможные сценарии атак. Также это позволяет ИИ выявлять какие-либо дыры в защите или уже имеющиеся аномалии в системе, что позволяет эффективно и успешно пресекать атаки. Хоть ИИ сам по себе и не выступает основным средством защиты от внешних угроз, но является отличным инструментом для IT-специалистов компаний.

2. Анализ сетевой безопасности. Данный аспект позволяет выявлять и разделять все типы подключений на санкционированные и несанкционированные. Данная особенность имеет большую пользу для больших компаний, где следить сразу за всеми подключенными пользователями. ИИ в этом случае уменьшает как процент ручного труда, так и исключает человеческий фактор, который может стать источником множества проблем.

3. Поведенческий анализ. Постоянный мониторинг за действиями пользователей. Отклонение от одной из установленных моделей поведения

---

[1] С.Э. Мерзляков «К вопросу о понятии информационной безопасности» - https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-informatsionnoy-bezopasnosti/viewer

[2] Научная статья блога компании Neuro.net « Как ИИ кибербезопасность усиливает: новые тренды и возможности» - https://habr.com/ru/companies/neuronet/articles/645539/

задействует алгоритм защиты. Такой анализ позволяет работать вообще почти со всеми типами информации. Например, именно этот тип анализа определяет местоположение пользователя при его попадании на сайт и соответственно вызывает блокировку в случае если местоположение внесено в черный список. Однако стоит заметить, что для такой работы специалистам компании необходимо загружать определенную, допустимую модель поведения, что добиться наиболее эффективного процесса.

4. Обнаружение мошенников. Наиболее важной проблемой является защита денежных средств пользователей банка. Однако даже здесь преуспел искусственный интеллект. ИИ допускает как можно меньше ложных защитных решений, что делает его наиболее гибким и эффективным.

Разобрав все вышеизложенные функции ИИ в обеспечении информационной безопасности можно сделать выводы, что искусственный интеллект является лишь инструментом, который требует умелого пользования в руках IT специалистов компании.

Однако можно заметить, что в некоторых моментах по обеспечению информационной безопасности ИИ предпринимает абсолютно самостоятельные действия. Например многие могли столкнуться с автоматизированной генерации криптографических ключей, которые устраняют необходимость в ручном вводе такового. Также можно заметить, как ИИ активно использует динамические[1] и квантово-устойчивые[2] типы шифрования. Также ИИ активно управляет доступом. Здесь подразумевается аутентификация пользователя, производящаяся с помощью анализа его поведенческого шаблона. Не менее важную роль могут играть адаптивное управление доступом и выявление аномалий. Из таких самостоятельных функций у ИИ можно выделить ряд преимуществ, таковыми являются: повышенная безопасность с помощью автоматизации и улучшения процессов шифрования, удобство применения ИИ, соответствие нормативным требованиям GDPR[3] и PCI DSS[4], повышенная защита от взлома и экономия затрат, поскольку серьезно

---

[1] Динамическое шифрование — ИИ корректирует шифрование в реальном времени и отталкивается от контекста исходящих угроз, тем самым повышая безопасность в разы. - https://dev.abcdef.wiki/wiki/Dynamic_encryption

[2] Квантово- устойчивое шифрование — ИИ сам разрабатывает и внедряет определенный алгоритм шифрования, который будет устойчив к квантовым видам атак. - https://na-journal.ru/5-2023-informacionnye-tekhnologii/5236-

[3] GDPR – регламент ЕС, который обновляет и расширяет раннюю директиву о защите данных (DPD) -izuchenie-vozmozhnostei-i-ogranichenii-kvantovo-ustoichivyh-kriptograficheskih-algoritmov#:~:text=Квантово-устойчивые%20криптографические%20алгоритмы%20—%20новое,задачи%20факторизации%20и%20дискретного%20логарифмирования https://ru.wikipedia.org/wiki/Общий_регламент_по_защите_данных

[4] PCI DSS – стандарт безопасности данных платежных карт, учрежденный международными платежными системами Visa, MasterCard, American Express. - https://ru.wikipedia.org/wiki/PCI_DSS

автоматизирует выполнение задач и снижает операционные расходы. Однако это не все преимущества ИИ в обеспечении информационной безопасности.

Также одной из важных сфер применения ИИ является как раз сфера образования в области ИБ, использование которого описано в научной статье Петренко Д.П. «Влияние искусственного интеллекта и нейросетей на цифровую образовательную среду: угрозы и возможности»[1], на основе описанной в источнике информации можно понять, что с помощью применения искусственного интеллекта активно удается строить персонализированные программы обучения, которые учитывают все конкретные потребности учащихся. У таких систем персонализированного обучения, согласно информации в источнике, можно выделить следующие типы:

1. Индивидуальные учебные планы, адаптированные под ученика с помощью оценки имеющихся знаний и генерации всех учебных процессов специально для достижения конкретных целей направленных на прогрессирование ученика.
2. Адаптивные уроки, так же корректируют свою сложность на основе уже имеющихся показателей учащегося
3. Персонализированные рекомендации, которые нейросеть предоставляет основываясь на выводах приведенных из результатов обучения.
4. Виртуальные тренеры, позволяют отвечать на вопросы учащегося и регулировать сам процесс обучения исходя из требований учащегося.

Исходя из данных типов систем обучения можно выделить ряд преимуществ, который делает как можно эффективнее процесс обучения и помогает освоить определенные темы в кратчайшие сроки. Преимуществами здесь можно выделить: персонализацию, адаптивность, автоматизацию и мониторинг и анализ. Как уже можно было заметить использование ИИ открывает множество возможностей для создания персонализированных программ обучения в области информационной безопасности. С его помощью получается серьезно повысить эффективность обучения, обеспечить увлеченность учащихся и достичь хороших результатов обучения, что в принципе положительно сказывается на системе образования.

Так же не стоит забывать, что помимо обеспечения самой безопасности и применение в образовательной сфере искусственный интеллект также используют для повышения осведомленности пользователей о кибер угрозах. Достижения нужного уровня осведомленности достигается с помощью выполнения следующих функций:

Персональные предупреждения, основанные на распознании уязвимости в системе и появление предупреждение для пользователя, уведомляющее его о присутствии данной проблемы.

---

[1]Петренко Д.П. «Влияние искусственного интеллекта и нейросетей на цифровую образовательную среду: угрозы и возможности» - https://www.sgu.ru/sites/default/files/textdocsfiles/2023/12/12/petrenko_d.p.pdf

Проактивное образование, которое используя чат-ботов, инфографику и викторины позволяет наиболее лучшим образом объяснять поступающую информацию.

Симуляция кибератак, которая в первую очередь позволяет находить многие уязвимости в системе, а также выработать способы защиты и спроектировать наиболее эффективную систему защиты от кибератак.

Применение данных функций помогает создавать наилучшие условия в сфере информационной безопасности, обеспечивая высокую эффективность работы всех систем.

Подводя итоги исследования, можно сделать некоторый выводы, что ИИ имеет вполне себе серьезное влияние в сфере защиты информации с помощью выполнения некоторого ряда функций и регулярного машинного обучения, что делает применение искусственного интеллекта — «защитной системой будущего», имеющую следующие положительные тендеции

- Всеобъемлющее использование нейросетей для автоматизации решения задач по обеспечению безопасности во всех сфера, где непосредственно имеется надобность.
- Интеграция их в системы безопасности при помощи создания адаптивных систем безопасности, и выполнения ими функций анализа данных пользователей и предоставления аналитики и рекомендаций для улучшения работы.
- Использование для обнаружения и предотвращения всех имеющихся типов атак, которые могут нанести высокий урон информационной безопасности.
- Повышение безопасности интернет вещей (IoT[1])

Таким образом интеграция ИИ в сферу информационной безопасности имеет положительные тендеции к развитию в будущем и решающее значение для повышения эффективности мер, обеспечивающих наивысший уровень безопасности.

Литература

1. Э.М. Продайков «Современное состояние искусственного интеллекта» - https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-iskusstvennogo-intellekta/viewer.

2. С.Э. Мерзляков «К вопросу о понятии информационной безопасности» - https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-informatsionnoy-bezopasnosti/viewer.

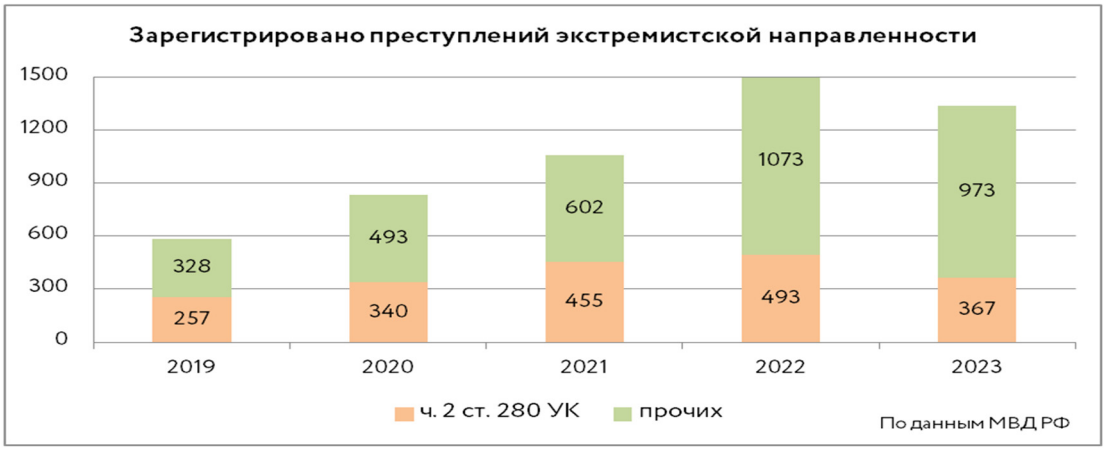
3. Петренко Д.П. «Влияние искусственного интеллекта и нейросетей на цифровую образовательную среду: угрозы и возможности» - https://www.sgu.ru/sites/default/files/textdocsfiles/2023/12/12/petrenko_d.p.pdf.

[1] Internet of Things (IoT) – это множество физических, подключенных к интернету и обменивающихся данными. - https://habr.com/ru/companies/otus/articles/549550/

Гаевский Александр Дмитриевич,
доцент кафедры оперативно-розыскной
деятельности и специальной техники
Донецкого филиала ФГКОУ ВО
«Волгоградская академия МВД России»

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИСТСКИМ ПРЕСТУПЛЕНИЯМ, КОТОРЫЕ СОВЕРШАЮТСЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Согласно официальной статистике МВД РФ, число зарегистрированныхованных в 2023 году преступлений экстремистской направленности составило 1340 (-14,4 % к 2022 году; заметим, однако, что в 2022-й характеризовался ростом поэтому показателю аж на 48,2 % по сравнению с 2021-м)[1].



В январе 2024 года было зафиксировано 134 преступления, имеющих экстремистскую направленность. Увеличение количества зарегистрированных преступлений наблюдалось в 36 регионах РФ, в то время как снижение было отмечено в 49 регионах.

Проблема борьбы с экстремизмом в Российской Федерации в последнее время превратилась в одну из первоочередных задач общества и государства, поскольку экстремизм, учитывая кризисную и взрывоопасную обстановку на Украине, стал достигать пределов, реально угрожающих национальной безопасности России.

Разумеется, в течение продолжительного времени проблема борьбы с экстремистскими преступлениями, а тем более, которые совершаются с использованием информационных технологий является одной из самых актуальных сфер как для внутренней безопасности России, так и на международ-

---

[1] Статистика и аналитика [Электронный ресурс]. – Режим доступа: https://мвд.рф/dejatelnost/statistics

ной уровне. Экстремистские преступления проявляются в различных формах, включая религиозные, политические, этнические, идеологические и другие аспекты. Очевидно, эти антиобщественные явления оказывают отрицательное воздействие не только на государство, но и на общество в целом, влияя на его нормальную жизнедеятельность.

Особенно в последнее время, фактором, который обуславливает рост экстремистских преступлений, является развитие информационных технологий (далее – ИТ). Следует отметить, что число преступлений, с использованием информационных технологий, совершенных несовершеннолетними, выросло с 2020 года в 74 раза. В 2020 году это количество было 54 преступления, а в 2023 году уже зафиксировали более 4 тыс. таких преступлений. Это свидетельствует о том, что технологии развиваются, вовлечение в цифровую криминальную среду несовершеннолетних тоже развивается[1].

Информационные технологии могут быть разных видов к наиболее типичным возможно отнести: Internet-технологии (сетевые); компьютерные технологии (аппаратные средства, программное обеспечение); мультимедиа сетевые технологии, телеконференция, телевидение, системы поддержки принятия решений, добыча данных ИД (Data mining), искусственный интеллект (ИИ), экспертные системы (ЭС), нейронные сети, генетические алгоритмы, виртуальная реальность, системы поддержки работы группы, имитационные системы и другие.

Проблемами преступности в области новых информационных технологий занимались такие ученые, как С.А. Абакумов, Б.В. Вехов, В.А. Голубев, А.Ф. Долженков, А.В. Касаткин, В.Е. Козлов, С.С. Овчинский, М.Г. Щербаковский и другие. В разные годы общим проблемам применения средств специальной техники в ОРД посвящены труды А.М. Бандурки, Р.С. Белкина, Д.И. Биднякова, Г.М. Бирюкова, И.П. Казаченко, В.П. Межевого, В.А. Биляева и т.д.

Для эффективной борьбы с экстремизмом предлагается использовать комплексный подход, который позволит предупредить конкретные преступления экстремистской направленности с использованием ИТ, соответственно, усовершенствовать процесс борьбы с экстремистскими преступлениями, которые совершаются с использованием информационных технологий.

В соответствии со ст. 1 Федерального закона от 25 июля 2002 года № 114-ФЗ (ред. от 14.02.2024 №15-ФЗ) «О противодействии экстремистской деятельности», под экстремистской деятельностью общественных и религиозных объединений, либо иных организаций, либо средств массовой информации, либо физических лиц по планированию, организации, подготовке и совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности Российской Федерации и т.д.

---

[1] За последние 4 года дети совершили почти 4 тысячи ИТ-преступлений [Электронный ресурс]. – Режим доступа: https://rusvesna.su/news/1714128128

Серьезная опасность экстремизма представляется не только относительно безопасности и стабильности, но также законности, демократии и правам человека, проявление экстремизма выступает катализатором развития организованной преступности и незаконных вооруженных формирований, которые стремятся к свержению законной власти или нарушению территориальной целостности страны и т.д.[1]

В России молодежный экстремизм и интернет-экстремизм очень распространены в настоящее время. Эти виды экстремизма особенно опасны, потому что молодежь более подвержена влиянию различных экстремистских идей и концепций. Интернет сегодня оказывает сильное влияние на мировоззрение людей, особенно на молодежь. Экстремистские материалы в виде текстов, графических изображений и видеоизображений активно распространяются в онлайн-ресурсах и негативно влияют на молодых пользователей.

Противодействие онлайн-экстремизму уже на сегодня, является одной из приоритетных задач МВД РФ. Эффективная борьба с такой деятельностью возможна только при тесном сотрудничестве с разработчиками и провайдерами сайтов по блокированию экстремистской информации. Кроме того, необходимо улучшить взаимодействие с общественностью для осуществления работы по разъяснению населению и получению информации о сайтах и материалах экстремистского содержания»[2].

Считаем также целесообразным, отметить, что объект преступлений экстремистской направленности не является однородным и имеет специфику в силу многообразия форм экстремистской деятельности.

Согласно судебно-следственной практике, экстремистские преступления в 97% случаев совершаются лицами мужского пола, так И.В. Саличевой была проведена научно-исследовательская работа по выявлению возрастных категорий лиц, которые совершают экстремистские преступления. Результаты следующие: совершение экстремистских преступлений лицами до 18 лет – 24 %, с 18–25 –57 %, с 25–30 – 8 %, с 30–40 – 6 %, после 40 – всего 5%.

Из этого сделаем вывод, что преступниками-экстремистами чаще всего являются молодые люди, у которых жизненный опыт еще недостаточен и отсутствуют стабильные взгляды относительно происходящих явлений и событий.

Так, студент первого курса заочной формы обучения колледжа мостостроения и гидротехники, разместил на своей личной странице «ВКонтакте» комментарий «Почему бы не устроить хлопковый холокост?», возбуждая ненависть и вражду к русским как этнической группе и русским патриотам

---

[1] Давыдов О. В. Транснациональные преступления экстремистского характера как объект криминалистического исследования // Известия Тульского государственного университета. Экономические и юридические науки. 2015. N 1-2. С. 51.

[2] Валеев А.Х. Борьба с проявлениями экстремизма в сети Интернет // Бизнес в законе. Экономико-юридический журнал. 2011. N 6. С. 127.

как социальной группе и совершая акты насилия.[1] Как правило, преступники являются студентами или выпускниками образовательных учреждений, находятся без работы или по каким-то причинам не могут устроиться на работу. Заметно, что экстремистские преступления в меньшей степени совершаются в состоянии алкогольного опьянения.

Так, Волгоградский областной суд вынес приговор в отношении одного из организаторов взрывов, произошедших в апреле 2011 года у зданий ГИБДД УМВД России по г. Волгограду и Волгоградской академии МВД России. Экстремисту был вынесен обвинительный приговор с лишением свободы на 12 лет. Его деяния были предопределены идеологической ненавистью. Преступления, вдохновленные экстремистской идеологией, отличаются особым характером. Их специфика определяется не только самим актом преступления, но и выражениями, которые могут быть произнесены во время его совершения. Это могут быть призывы к нетерпимости на расовой, религиозной или националистической основе. После совершения преступления экстремист может оставить характерные националистические надписи, предметы или печатную продукцию. Они могут свидетельствовать о причастности к экстремистским группировкам и подтверждать, что преступление было совершено по их националистическим или религиозным мотивам.

Активные участники экстремистских групп с экстремистской идеологией, ведут массовую вербовочную и агитационную работу в интернете, распространяя материалы через «репосты» и отвергая свою вину, часто избегая наказания и получая свободу действий. Именно поэтому при обнаружении экстремистской информации в интернете необходимо тщательно изучать контакты, репосты, высказывания и комментарии, а также контекст и аудиторию, чтобы полностью понимать суть их действий.

Криминальные формы проявления молодежного экстремизма являются объектом повышенного внимания со стороны правоохранительных органов. Согласно ФЗ «О противодействии экстремисткой деятельности» от 25 июля 2002 г. № 114, очень важно определение экстремистских материалов во время публичных призывов к экстремистской деятельности лиц, совершающих данное деяние, могут использовать и распространять экстремистские материалы. Федеральный перечень экстремистских материалов публикуется на официальном сайте Минюста РФ и на настоящее время насчитывает 5424 наименований данных материалов.

На основании Закона РФ от 27 декабря 1991 г. N 2124-I «О Средствах массовой информации», под средством массовой информации следует понимать «…периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)».

---

[1] Погодин И.В. Доказывание по делам о преступлениях экстремистской направленности: автореф. дис. канд. юрид. наук 12.00.09. М.: Изд-во МПГУ, 2012. 22 с.

Широкое вовлечение молодежи в экстремистские организации и движения объясняется не только неудовлетворенность материальной стороной жизни. Снижение идеологической составляющей в воспитательном процессе привело к утрате частью молодежи нравственных ориентиров. Традиционные для российского менталитета нравственные ценности, такие как патриотизм, подверглись широкомасштабной деструктивной обработке извне (нередко принимавшей характер манипуляции общественным сознанием). Именно молодежь не способная критически подходить к содержанию публикаций в СМИ ввиду отсутствия жизненного опыта оказалась наиболее подверженной такому влиянию.

В настоящее время, следует отметить, что в сети Интернет в соответствии с действующим законодательством является средством массовой информации. Понимание особенности статуса СМИ в интернете, в том числе распространение с помощью сети Интернет экстремистских материалов, надо для правильной квалификации преступления, предусмотренного ст. 280 УК РФ, ст. 282 УК РФ, 282.1 и 282.2 и 282.3 УК РФ. [1] В применении к преступлению, предусмотренному ст. 282 УК РФ, объективную сторону преступления составляют действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц. Статьи 282.1 и 282.2 УК РФ, устанавливают ответственность за организацию деятельности экстремистского сообщества и экстремистской организации. Основные проблемы при толковании диспозиции данных статей заключаются в понимании «экстремистского сообщества» и «экстремистской организации» как организованных преступных структур направленных на совершение преступлений экстремисткой направленности, их соотношения и отграничения друг от друга. Если проводить анализ ст. 282.1 и 282.2 УК РФ то вывод можно сделать следующий, что основным различием является то, что деятельность экстремистской организации признается преступной с момента вступления в законную силу соответствующего решения суда. По факту вступления в законную силу решения суда о запрете деятельности организации в связи с осуществлением экстремистской деятельности есть ничто иное, как момент преобразования, когда законно созданное предприятие либо организация в любой организационно правовой форме превращается в экстремистское сообщество.

Статья 282.1 УК РФ предусматривает ответственность за совершение одного из трех самостоятельных преступлений указанных в диспозиции, а именно:

- создание экстремистского сообщества, а равно руководство таким сообществом;

---

[1] Борисов С.В. Новеллы уголовного законодательства в сфере противодействия экстремизму: критический анализ / С. В. Борисов, А. А.Чугунов. // Современное право. -2015. - № 4. - С. 101 -105) // [Электронный ресурс] Информационно-справочная Система «Консультант Плюс» - Электрон.дан. - URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=87189

- склонение, вербовка или иное вовлечение лица в деятельность экстремистского сообщества;

- участие в экстремистском сообществе.

Самое большое затруднение вызывает толкование склонения, вербовки, иного вовлечения в экстремистское сообщество, потому что отсутствует какое-либо законное определение данных форм осуществления объективной стороны составов преступления, предусмотренных, ст. 282.1, 282.2 и и 282.3 УК РФ УК РФ[1]. Вопрос научных дискуссий современных российских ученых отмечены в научных работах по вышеуказанным статьям УК РФ.[2]

Здесь же имеет смысл отметить, что в уголовно-правовой науке среди авторов отсутствует единое понимание участия в экстремистском сообществе, выделяются активные и пассивные формы такого участия. Законодатель в Постановлении Пленума ВС РФ от 28 июня 2011 г. N 11 "О судебной практике по уголовным делам о преступлениях экстремистской направленности" уточнил, что под участием в экстремистском сообществе надлежит понимать вхождение в состав такого сообщества с намерением участвовать в подготовке или совершении одного или нескольких преступлений экстремистской направленности, что само по себе предполагает вопрос, как квалифицировать деяние, если лицо вступило в сообщество без намерения совершать экстремистские преступления, как узнать, что у лица имеется такое намерение. По данному вопросу Пленум каких-либо разъяснений не дает.

Однако в вышеуказанном Постановление Пленума Верховного суда РФ в п. 16 говорится, что под участием в экстремистском сообществе надлежит понимать вхождение в состав такого сообщества и участие в подготовке к совершению одного или нескольких преступлений экстремистской направленности и непосредственное совершение указанных преступлений, а также выполнение лицом функциональных обязанностей по обеспечению деятельности такого сообщества (финансирование, снабжение информацией, ведение документации и прочее.). Следовательно, можно полагать, что законодатель указывает, что участие в экстремистском сообществе охватывает большую границу, указывая под видом формы деятельности такой преступной функции и финансирование экстремистского сообщества либо организации. На основании сказанного, мы можем констатировать, что при финансировании экстремистского сообщества, преступное лицо должно получить ответственность по реальной совокупности преступлений, как за финансирование, так и за участие в экстремистском сообществе. Получается, что есть несколько вариантов решения этой проблемы.

---

[1] Ульянова, В.В. Финансирование экстремистской деятельности: анализ законодательных новелл // Общество в эпоху перемен: современные тенденции развития. Сибирский институт управления – филиал РАНХиГС. – Новосибирск : СибАГС, 2014. – С. 432–434.

[2] Холоимов Г.С. Уголовно-правовая характеристика финансирования экстремистской деятельности // Научная перспектива. – 2014. – № 8. – С. 74–75.

Резюмируя вышесказанное, следует отметить, что успех противодействия экстремистским преступлениям, которые совершаются с использованием информационных технологий зависит от своевременного обнаружения противоправных деяний экстремистского характера, а также лиц, их совершающих, и их правильной уголовно-правовой квалификации. На практике, к сожалению, не всегда уделяется должное внимание правовой квалификации этих деяний. В результате этого они не получают правильной правовой оценки, что в свою очередь приводит к безнаказанности виновных.

Таким образом, в качестве основных направлений реализации противодействия преступлениям экстремистского направленности правоохранительными органами РФ и их подразделениями предлагаются:

– с целью профилактики вышеуказанных преступлений систематично проводить разъяснительную работу о противодействии экстремизма в молодежной среде общества, использование всех возможностей для расширения доступности для молодежи досуговых учреждений. Формирование у молодежи правильного отношения к труду, здоровью, обществу и государству, активная пропаганда идей патриотизма, любви к Родине, а также безысходности экстремизма;

– принятие реальных мер, направленных на ограничение разрушительного воздействия некоторых средств массовой информации в сети Интернет; периодический мониторинг СМИ в сфере экстремистской направленности с целью выявления призывов к осуществлению насильственных и иных противоправных действий в ходе проведения массовых мероприятий, либо к проведению собственно экстремистских акций;

– оперативное (своевременное и квалифицированное) их пресечение молодежного экстремизма с использованием информационных технологий;

– управление силами и средствами ОВД и тактику действий, при обострении социально-политической обстановки, вызванном резким ростом криминальных проявлений молодежного экстремизма с использованием информационных технологий;

– оперативно-розыскное обеспечение таких действий в противодействии молодежному экстремизму с использованием информационных технологий;

– организация взаимодействия и координацию усилий структур, участвующих в предупреждении и пресечении криминальных проявлений молодежного экстремизма с использованием информационных технологий.

– разработка новых составов преступлений (с учетом специфики как уголовной ответственности) и включение соответствующих правовых норм в действующий УК РФ в противодействии молодежному экстремизму с использованием информационных технологий;

– организовать подготовку специалистов на базе Донецкого филиала Волгоградской академии МВД РФ, способных успешно осуществлять борьбу с экстремистскими преступлениями, которые совершаются с использованием информационных технологий.

Григорусь Людмила Николаевна,
старший преподаватель кафедры
гуманитарных и социально-экономических дисциплин
Крымского филиала Краснодарского университета МВД России

Эмиров Эрлен Нусритович,
Курсант Крымского филиала
Краснодарского университета МВД России

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время применение цифровых технологий затрагивается всеми сферами жизни общества. Деятельность человека, в большинстве случаев, связана с информационными технологиями, и существование таких терминов как «Цифровизация» или «цифровая трансформация» должен знать и понимать каждый.

Определение цифровизации, в зависимости от сферы деятельности может иметь различные значения. Однако, цифровизация представляет собой внедрение цифровых технологий и новых алгоритмов, облегчающих жизнедеятельность человека, применяемая не только в сфере бизнеса и производства, но также в политической, экономической, культурно-образовательной и правоохранительной деятельности [3, стр. 187-189].

Сотрудники органов внутренних дел (далее ОВД) осуществляют деятельность, направленную на раскрытие, пресечение и предупреждение преступлений, а также деятельность по розыску лиц, совершивших преступление, укрывающихся от исполнения наказания и без вести пропавших лиц. Необходимость использования сотрудниками ОВД цифровых технологий возникает в связи с ростом преступлений в сфере информационных технологий. Это касается области экономических преступлений, поскольку злоумышленник обладает достаточно высоким интеллектом, знанием различных программ и процессов.

Использование преступниками цифровых технологий возлагает дополнительные обязанности на сотрудника полиции по их изучению. Для решения данной проблемы создается комплекс систем, состоящий из специальной вычислительной техники и специального программного обеспечения.

Федеральный закон «О полиции» № 3 от 07.02.2011 года в ст. 11 устанавливает в качестве одного из принципов деятельности полиции возможность использования достижений науки и техники, современных технологий и информационных систем [1, ст. 11]. Таким образом, на уровне законодательства закрепляется использование цифровых технологий в правоохранительной деятельности. Благодаря этому в 2012 году МВД утверждена концепция создания единой системы информационно-аналитического обеспечения де-

ятельности (далее ИСОД) МВД России, которая представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов, а также средств связи и передачи данных, необходимых для обеспечения служебной деятельности. ИСОД МВД России, принятая утверждением Правительства РФ в 2014 году, затрагивает, в том числе, деятельность отдельных ведомств, в том числе, тыловых подразделений, кадровых и материально-технических. Данная система является центром обработки и хранения информации из полученных источников видеофиксации. Например, в настоящее время, существует АИС «Безопасный город», которая позволяет предупреждать преступления и административные правонарушения, такие как массовые беспорядки.

Сотрудники правоохранительных органов расследуя преступления, осуществляют производство следственных действий, предполагающих работу с цифровыми технологиями. Во-первых, информация, собранная путем применения цифровых технологий может выступать в качестве доказательств по уголовному делу. Однако, предоставлять такую информацию можно исключительно на электронном носителе: дискет, сервер, флеш-карта и т.д. Во-вторых, для того, чтобы изучить электронные доказательства и приобщить их к материалам уголовного дела необходимо наличие и использование специальных программ и оборудований: ноутбук, компьютер и т.д.

Нормативно-правовая база, используемая сотрудниками правоохранительных органов, устанавливает правомерность применения ими цифровых технологий. Так, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в котором устанавливаются основные понятия, используемые в настоящем законе, а также реализацию права на доступ к информации и обеспечение защиты информации от неправомерного доступа. Кроме Федерального закона, сотрудники ОВД руководствуются Уголовно-процессуальным Кодексом Российской Федерации, который не имеет определения цифровых технологий, но допускает применение электронных носителей информации, которых в дальнейшем можно отнести к вещественным доказательствам либо к иным документам [4, с. 64].

Тем не менее существует проблематика качественного анализа и обработки информации, и количественного фактора. Качественный фактор предусматривает недостаток квалифицированных кадров, из-за чего процесс обработки информации замедляется, и как следствие, объемы полезной информации не реализуются сотрудниками ОВД в должной мере. Именно поэтому, необходимо повышать квалификацию сотрудников в области использования цифровых технологий, поскольку это облегчает некоторые задачи их деятельности и повышает качество и достоверность обработки данных. Количественный фактор вызван недостатком информационно-технического обеспечения, что также затрудняет сотрудникам ОВД осуществлять свою деятельность с использованием цифровых технологий.

МВД России состоит из подразделений - Государственная инспекция безопасности дорожного движения (далее ГИБДД) является самостоятельным структурным подразделением центрального аппарата МВД России. Деятельность, проводимая сотрудниками ГИБДД, направлена на осуществление федерального государственного надзора и специальных разрешительных функций в области безопасности дорожного движения, а именно контролем за транспортными средствами, их водителями, регулированием дорожного движения, проведением профилактической работы и расследованием дорожно-транспортных происшествий. В обязанности подразделения ГИБДД также входит выдача и проверка документов, связанных с управлением автотранспортными средствами.

Для повышения эффективности деятельности ГИБДД, в соответствии с Приказом МВД РФ от 05.02.2016 N 60 «О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции», предоставляется возможность аккумулировать информацию о зарегистрированных транспортных средствах, выданных водительских удостоверений, административных правонарушениях и т.д.[2, п. 1] Следует отметить, что до принятия указанного Приказа МВД России все эти данные находились в несогласованности, поскольку сохранялись в различных сервисах ГАИ. Следствием служили постоянные сбои системы, задержки и как итог неэффективность работы сотрудников ГИБДД.

В настоящее время сотрудники ГИБДД активно используют цифровые технологии для улучшения работы и увеличения эффективности проверок и контроля на дорогах. Им также предоставляются государственные услуги, реализуемые через Единый портал государственных услуг (далее ЕГПУ):

- извещение граждан РФ о тех или иных обстоятельств, например, предоставление или замена водительского удостоверения;

- предоставление данных о нарушении ими ПДД, а также об аннулировании их водительских документов;

- предоставление иных сведений, затрагивающих права и интересы участников дорожного движения и т.д.

Таким образом, несмотря на то, что законодательство в области применения сотрудниками ГИБДД цифровых технологий достигло больших результатов по обеспечению выполнения ими задач и функций, следует расширять нормативно-правовую базу в сфере цифровых технологий, а также урегулировать цифровизацию предоставления государственных услуг ГИБДД.

Например, для получения большей информации о гражданине, имеющим водительское удостоверение, следует установить его цифровой паспорт. В данном случае, цифровой паспорт водителя будет иметь необходимые сведения о лице, как о добросовестном участнике дорожного движения. Так, данные, предоставляемые в цифровом паспорте зарегистрированного водителя, представляют работодателям возможность заранее просматривать информацию о них в качестве участника дорожного движения.

Это необходимо, например, в тех случаях, когда лицо, имеющее водительское удостоверение, желает управлять транспортным средством, которое ему не принадлежит (регистрация на работу автотранспортного предприятия, где необходимо управлять транспортным средством), данные о нем могут просматриваться работодателем. Также в тех случаях, когда водитель находится в дороге, соблюдает ли он правила дорожного движения. Это является необходимым, так как при совершении ДТП или нарушении ПДД, работодатель буде располагать достоверной информацией. Цифровой паспорт водителя должен находиться в ГИБДД, и по запросу работодателя, может предоставляться с их разрешения. Также, подразделения ГИБДД с помощью цифрового паспорта смогут дать правильную оценку, при совершении водителем правонарушения или преступления.

Таким образом, использование цифровых технологий структурными подразделениями ОВД И ГИБДД является необходимым. В связи с совершенствованием технологий, обязанностей у сотрудников становится все больше и для этого необходимо принимать меры, которые предложены в данной статье и считаются наиболее приемлемыми для решения, стоящих перед подразделениями ОВД и ГИБДД, проблем.

Литература

1. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // СПС «Гарант»
2. Приказ МВД РФ от 05.02.2016 № 60 «О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции» // «Гарант»
3. Елохина, Э. Э. Цифровизация современного социума: достоинства и угрозы / Э.Э. Елохина. – Текст : непосредственный // Молодой ученый. – 2023. – № 24 (471). – С. 187-189.
4. Противодействие правонарушениям, совершаемым с использованием информационных технологий: сборник статей по материалам научно-практической конференции // отв. ред. В.В. Казаков ; сост. К.А. Комогорцева; Университет прокуратуры Российской Федерации; – М. : МФЮА, 2021. – С. 64.

Датиев Ацамаз Аланович,
преподаватель
Краснодарского университета МВД России

Курочкина Диана Владимировна,
слушатель
Краснодарского университета МВД России

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ АТАК КЛАССА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ПРИМЕНЯЕМЫХ В КИБЕРТЕРРОРИЗМЕ

Современные тенденции диктуют свои правила, согласно которым многие государственные и коммерческие организации разрабатывают информационные системы, доступные в сети Интернет. Благодаря этому повышается удобство и эффективность взаимодействия как подразделений самой организаций, так и пользователей, обращающихся к этим организациям. В качестве подобных информационных систем можно привести в пример следующие сервисы: портал государственных услуг Российской Федерации, портал федеральной налоговой службы, платформа Домклик, ЕИС Закупки и др. Подобного рода организации аккумулируют критически важной информацией.

Согласно отчету Национального координационного центра по компьютерным инцидентам (НКЦКИ) [1], ежедневно на информационные российские ресурсы фиксируется более 170 комплексных компьютерных атак. Среди совершаемых кибератак весомая доля приходится на критическую информационную инфраструктуру государства. Тем самым, можно сказать, что подобного рода кибератаки выходят на принципиально новый уровень, называемый кибертерроризмом.

Кибертерроризм – это угроза глобальной безопасности, возникающая при совершении киберпреступлений, затрагивающих интересы национальной безопасности. Кибертерроризм может использоваться для уничтожения или нанесения ущерба критической инфраструктуре цели, в ходе достижения политических или идеологических мотивов преступников.

К видам кибератак, реализуемым в ходе совершения акта кибертерроризма относят:

- Вредоносные программы, используемые для атак на военные системы, транспортную сеть или гражданские объекты;
- DoS-атаки типа «отказ в обслуживании», направленные на отключение узлов критической информационной инфраструктуры жертвы;
- Методы социальной инженерии, используемые для получения конфиденциальной информации (сведения, содержащие государственную тайну, логины, пароли).

Социальная инженерия – это совокупность методов взлома информационной системы, использующих человеческие слабости (доверчивость, мнительность, чувство страха) в качестве рычага давления.

К методам социальной инженерии относятся [2]:

1. Фишинг – совокупность методов кибератак, использующих заранее подготовленный сценарий действий, согласно которым киберпреступник выдает себя за надежный источник, которому можно доверять. В качестве механизма воздействия на жертву могут использоваться письма от банка, звонки от лица сотрудников органов исполнительной власти, обращения рекламного характера. Все эти методы объединяет попытка маскировки исполнителя кибератаки под видом легитимного представителя той или иной организации.

2. Фарминг – метод социальной инженерии, использующийся при сборе важной информации о жертве для реализации более результативной кибератаки. Часто данный метод используется злоумышленником в рамках киберразведки.

3. Дорожное яблоко – частный случай методов кибератак, называемых «троянским конем». Злоумышленник оставляет материальный предмет (флеш-накопитель, смартфон) на видном месте в расчете на излишнее любопытство жертвы. Чаще всего в роли наживки выступают зараженные вредоносным программным обеспечением устройства.

В качестве возможных последствий реализации приведенных видов кибератак можно указать [3]:

- потерю критически важной документации;
- несанкционированный доступ к сведениям, содержащим государственную или иную тайну;
- критические повреждения, нанесенные аппаратному обеспечению информационной системы организации.

В целях предотвращения указанных последствий необходимо проверять источник поступившего запроса или сообщения. При появлении незнакомых устройств в зона рабочего места сотрудника, необходимо незамедлительно сообщать о них в отдел информационной безопасности организации или руководителю подразделения сотрудника.

Одним из аспектов, позволяющих предотвратить кибератаку можно отнести организационные методы [4], включающие в себя своевременное повышение квалификации сотрудников. Кроме того, актуальность состояния программного обеспечения, отвечающего за обнаружение проникновения во внутренний контур информационной системы позволит своевременно зафиксировать инцидент кибербезопасности. Но одним из самых оптимальных и надежных инструментов по предотвращению кибератак выделяют спам-фильтр. Корректно настроенный спам-фильтр обезопасит сотрудников организации от контактов со злоумышленниками и предотвратит утечку информации за пределы критической информационной инфраструктуры.

Таким образом, кибертерроризм, имеющий своей целью подрыв национальной, политической и идеологической безопасности страны, использующий развитые методы социальной инженерии может быть обезврежен благодаря комплексному подходу к безопасности.

Литература

1. Сетевое издание TAdviser. Число кибератак в России и в мире. https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире.

2. Ресурсный центр компании Kaspersky. Социальная инженерия – защита и предотвращение. https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks.

3. Алоева, А. А. Информационный терроризм - угроза национальной безопасности в условиях цифровизации / А. А. Алоева, И. А. Алоев, А. З. Жуков // Пробелы в российском законодательстве. – 2020. – Т. 13, № 6. – С. 197-201. – EDN IKPTLN.

4. Блог Яндекса. Безопасность в интернете/Нарушения. https://yandex.by/ support/webmaster/threats.html

Датиев Ацамаз Аланович,
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

Ручкин Тимур Русланович,
курсант
Краснодарского университета МВД России

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ДЕАНОНИМИЗАЦИИ ЛИЧНОСТИ ПРЕСТУПНИКА В ЗАЩИЩЕННОЙ СЕТИ TOR

За последние несколько десятилетий развитие информационных технологий не только упростило решение множества профессиональных задач, но и позволило традиционным видам преступной деятельности перекочевать в цифровую среду. Согласно статистической информации, опубликованной Главного управления правовой статистики и информационных технологий Генеральной прокуратурой Российской Федерации за январь – сентябрь 2020 года удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, от общего числа зарегистрированных преступлений составляет 23,6% [1]. Статистическая информация по распределению указанного соотношения приведена в табл. 1.

Таблица 1. Количество зарегистрированных преступлений, совершенных с использованием или применением различных информационных технологий

Применяемые технологии	**Количество**
Сеть Интернет	209671
Средства мобильной связи	155177
Пластиковых банковских карт	139597
Компьютерной техники	20795
Программных средств	7318
Фиктивных электронных платежей	931

Приведенные показатели наглядно демонстрируют тенденцию роста количества зарегистрированных преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Для расследования традиционных видов преступлений в структуре МВД России имеются проверенные временем эффективные методы раскрытия, что никак нельзя сказать про преступления, совершаемые в сфере информационных технологий. Данная ниша является молодой и нуждается в наполнении как теоретической базой знаний, так и практическими методами борьбы с преступностью.

Одной из основных проблем расследования преступлений, совершаемых в информационной сфере или с использованием информационных технологий является деанонимизация личности преступника. На данный момент имеется несколько проверенных, но не гарантирующих эффективного результата решения данной проблемы метода.

Для сокрытия своей личности в сети Интернет злоумышленники очень часто прибегают к услугам виртуальных частных сетей - VPN (англ. Virtual Private Network). Одним из методов, используемых в данном случае может выступать деанонимизация пользователей с использованием отпечатка браузера. Данный метод может показать свою эффективность благодаря тому, что используемый злоумышленником браузер отправляет на посещаемые им сайты информацию об устройстве и используемом программном обеспечении. К собираемой информации на стороне посещенных сайтов можно отнести user-agent, который может выглядеть следующим образом: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0. User-agent является программным элементом браузера, позволяющим идентифицировать каждого пользователя. Если получить доступ к остальной информации, являющейся частью отпечатка браузера, например, часовой пояс, размера экрана пользователя, язык и использовать их комплексно, то данный способ позволит значительно сократить выборку поиска устройства злоумышленника [2]. Преимуществом данного способа деанонимизации является то, что описанная механика функционирования браузера свойственна, в том числе, одному из самых популярных в киберпреступной среде браузеров – Tor-браузеру (сокр. от англ. The Onion Router)[3].

Таким образом, можно сделать вывод, что проблема деанонимизации злоумышленников в сети Интернет является крайне актуальной, по причине активного использования ими таких технологий, как VPN, proxy и Tor. Огромную роль в решении указанной проблемы сыграют новые методы деанонимизации, которые только предстоит разработать.

Литература

1. Состояние преступности в России за январь - сентябрь 2020 года. URL: https://epp.genproc.gov.ru/documents/1664002/56420425/состояние+преступности+в+россии.pdf.

2. Поздышев, Р. С. Деанонимизация личности преступника в сети Интернет / Р.С. Поздышев // Вестник Уральского юридического института МВД России. – 2022. – № 2(34). – С. 50-53. – EDN SUVXDN.

3. Tor. URL: https://ru.wikipedia.org/wiki/Tor.

Елагина Виктория Владимировна,
руководитель отдела системного анализа
ООО «НТЦ «Вулкан»

МЕТАВСЕЛЕННЫЕ. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ СФЕРЕ

Статья является более глубоким научным погружением в исследование проблем и научных идей, предложенных к обсуждению в статье «Метавселенные. Потенциальные угрозы безопасности в информационной и технологической сферах», опубликованной в журнале «Защита информации. INSIDE № 4'2024».

Целью настоящей статьи является информирование профессионально-заинтересованного сообщества о выявленных способах оказания негативного влияния на социум в виртуальных пространствах метавселенных.

Объектом исследования являются потенциальные угрозы безопасности со стороны метавселенных в информационно-психологической сфере, а также способы негативного воздействия, применяемые в виртуальных пространствах.

Для достижения поставленной цели проведен научный эксперимент с целью изучения контента метавселенных и способов его модерации. В ходе эксперимента было организовано взаимодействие с пользователями следующих сервисов: Roblox, VRChat, Second Life, Decentraland, Spatial, Meta Horizon Worlds. По результатам проведенной работы составлен перечень угроз со стороны метавселенных в информационно-психологической сфере, выявлены случаи пропаганды запрещенных на территории Российской Федерации идей и взглядов, а также иные способы оказания негативного воздействия на пользователей.

Основная аудитория метавселенных

В настоящее время ежемесячная аудитория активных пользователей метавселенных насчитывает около 400 млн. человек, большая часть которых – представители поколений Z[1] и Альфа[2]. Зумеры и Альфа – поколения, для которых компьютерные и сетевые технологии стали доступны с раннего детства, в связи с чем их психологическое состояние, когнитивные функции, а также способность воспринимать информацию имеют принципиальные отличия от других поколений, в частности:

1. Благодаря высокой степени погруженности в цифровые среды молодые люди могут иметь тенденцию к развитию путаницы в идентичности, когда реальная и виртуальная сущности человека кардинально отличаются, при этом обе воспринимаются как реальные [1], [2].

---

[1] Поколение Z («зумеры», «цифровые люди») – люди, родившиеся в 1997 – 2012 гг.

[2] Поколение Альфа (Alpha) – первое поколение, полностью родившееся в XXI веке.

2. Обладая с детства доступом к телевидению, интернету, компьютерным играм и в целом не фильтруемому контенту, средний американский подросток к 18 годам видит более 200 тыс. актов насилия [3], включая жестокие убийства. Также увеличилось число подростков, которые смотрят порнографические фильмы, в том числе для «просвещения» в вопросах сексуальности [4]. Проблема усугубляется широкой пропагандой ЛГБТК+ культуры. Тем самым меняются сексуальные предпочтения потребителей такого контента, подростки-юноши становятся асексуальными, предпочитают виртуальных девушек под управлением ИИ, теряют смысл личного общения. Популярными сексуальными темами становятся различные девиации, например, фембои (женоподобные мальчики) и фурри (сексуализированные антропоморфные животные) [5]. На повестке всерьез стоит возможное продолжение в виде легализации прочего девиантного поведения. На форуме ПМЭФ в 2024 г. детский омбудсмен М. Львова-Белова прокомментировала появление субкультуры фурри, в которой дети (подростки и молодые люди) переодеваются в животных: «Это не может не настораживать, на это нужно реагировать и принимать меры» [6].

3. Физическая половая зрелость у представителей поколения Z наступает раньше, чем это было со старшими поколениями, более того, в развитых государствах половое созревание наступает раньше, чем в отдельных странах Африки. При этом половая и психосоциальная зрелость тоже больше не совпадают. Это связано с разными факторами, в том числе с доступностью деструктивного контента [7], [8], [9]. [10], [11].

4. С середины 80-х годов XX века в развитых странах отмечается стагнация и падение уровня IQ1. Ученые отмечают, что это может быть связано с загрязнением воздуха, а также с тем, что молодежная культура становится более примитивной, а повсеместное распространение компьютеров ведет к сокращению чтения книг, ухудшению восприятия текстовой информации, туннельному мышлению, предпочтению видеоинформации, а также снижению вычислительных способностей [12], [13], [14], [15].

Таким образом, представители поколений Z и Альфа – основные потребители метавселенной – являются наиболее уязвимыми для деструктивного воздействия, которое может быть оказано в сервисах новых цифровых экосистем.

---

[1] Согласно эффекту Флинна с начала XX века уровень интеллекта (IQ) населения Земли регулярно рос, что могло быть связано с такими факторами, как улучшение уровня жизни, медицины и питания, доступность образования, а также нарастающая стимуляция нейронов человека в связи с распространением визуальных медиа (телевидение, интернет, видеоигры). Т.е. каждое последующее поколение находилось в реальности, все более нагруженной оптическими дисплеями, продвигаясь, в связи с этим, в возможностях головного мозга в визуальном анализе [19].

Угрозы в информационно-психологической сфере

Ранее были выделены следующие угрозы в информационно-психологической сфере, предлагаю рассмотреть их более глубоко и детальнее раскрыть аспекты их воздействия:

Радикализация общества (распространение экстремистских идей и взглядов)

Существует множество исследований о деятельности экстремистских организаций в социальных сетях [16], [17], [18]. Однако пространство метавселенных открывает больше возможностей, связанных, в т.ч. со сложностью модерации контента (например, использование агрессивного языка в чатах, комментариях и мессенджерах может быть выявлено с помощью работы систем машинного обучения, при этом потоковая фильтрация речи – более сложная задача, требующая значительных затрат вычислительных мощностей), различиями в законодательствах разных стран (например, «Организация украинских националистов» запрещена в РФ, однако не является экстремистсчткой в законодательстве других государств, из-за чего этот контент становится доступным гражданам Российской Федерации), а также с иммерсивным повествованием – возможностью создавать визуальный контент с определенной эмоциональной и смысловой нагрузкой.

Наличие экстремистских и ультраправых организаций выявлено в метавселенной VRChat, Second Life и Spatiel. Кроме того, такого рода контент найден в сервисе Roblox, однако благодаря более строгим правилам модерации и большому резонансу в СМИ он был оперативно заблокирован.

Появление новых скрытых каналов распространения запрещенной информации

Во многих метавселенных есть возможность создания «скрытых комнат» для общения и взаимодействия. В сервисах Spatiel и Decentraland, которые поддерживают блокчейн и использование NFT, предусмотрена функция Token Gating, когда доступ в локацию открывается только тем пользователям, которые обладают определенным NFT. А в VRChat и Second Life есть возможность создания приватных комнат, ключ доступа и разрешение на вход в которые распространяется лично автором. Таким образом, контроль за действиями и контентом в этих локациях становится практически невозможным, что открывает дополнительную возможность распространения информации о запрещенных веществах и способах их приготовления, детской порнографии и пр. [20]

Провоцирование деструктивной протестной деятельности.

Как было указано выше, метавселенные позволяют создавать разнообразные иммерсивные виртуальные пространства с авторским контентом, где можно в т.ч. организовывать проведение массовых встреч, проводить «репе-

тиции протестных акций и митингов», осуществлять работу с общественностью. Для этого пользователю достаточно создать локацию на определенную тему и украсить ее соответствующей символикой. Для более глубокого погружения и «реальной картинки» могут быть воссозданы карты городов, где пользователи смогут «отрепетировать» стачку или митинг, столкновение с полицией и определить «пути отхода».

Кроме того, подобного рода деятельность в метавселенных может быть использована для создания определенной повестки и привлечения более молодых поколений. В частности, в 2023 г. наравне с акциями в городах США и Европы, в Roblox прошли виртуальные митинги в поддержку Палестины.

Опасность такого инспирирования протестной деятельности заключается еще и в том, что распространение идей становится транснациональным, когда волнения могут быть подхвачены в разных точках мира, что создает иллюзию тотальной поддержки и вовлеченности, как это было, например, в метавселенной Second Life, когда украинскую символику можно было найти в самых неожиданных локациях и точках на карте. Примечательно, что с начала 2024 г. эта тенденция идет на спад.

Развитие синтетических и химических веществ для более глубокого погружения в метавселенную

Основной нерешенной в настоящее время задачей при погружении в пространство метавселенных является сложность с воссозданием реальных ощущений. Несмотря на то, что уже есть некоторые технологические решения, которые сглаживают разрыв между цифровым и реальным миром[1], они все еще несовершенны и имеют ограниченные возможности. Для более глубокого погружения и стимуляции ощущений и эмоций могут применяться различные способы воздействия на мозг, в т.ч. фармакологические, которые способны провоцировать реакции, сравнимые с эффектом употребления психоделиков. Учитывая возраст основной аудитории пользователей метавселенных, существует риск роста числа случаев приема запрещенных препаратов.

Способы воздействия на аудиторию в метавселенных

Влияние на сознание и убеждения пользователей метавселенных осуществляется классическими способами оказания информационно-психологического воздействия, а именно [22], [23]:

убеждение;
разъяснение;
информирование;

[1] Французская и испанская компании Ubisoft и OWO представили футболку с тактильной отдачей, которая передает игроку ощущения, испытываемые главным героем игры, например, дуновения ветра на коже или ранения от выстрела [21].

обсуждение;
сравнение;
воспитание;
содействие и поддержка;
изменение настроения;
формирование психологического фона;
распространение слухов;
дезинформация и пр.

Однако важно отметить, что в отличие от «классических» средств массовой информации и коммуникаций, метавселенные предлагают не просто просмотр «плоского контента», а непосредственное погружение и иногда участие в смоделированных событиях в т.ч. с помощью устройств виртуальной реальности. Согласно последним исследованиям, при погружении в виртуальную реальность у мозга возникают сложности с разграничением цифрового и реального опыта, а интенсивность эмоций соизмерима с реальными[1]. Таким образом классические способы воздействия могут быть усилены за счет воздействия на эмоции[2], поскольку пространство метавселенных позволяет моделировать любую виртуальную среду, которая может переносить пользователя в определенные события. Таким образом распространяются идеи и рассказы о событиях в эмоциональной субъективной авторской трактовке, а пользователям предлагается посетить непосредственно «место события». Подобное погружение вызывает эмоциональную вовлеченность и сильные переживания, что снижает способности мозга к объективному восприятию информации и определения ее достоверности.

Еще один усиливающий фактор – возможность организации игрового взаимодействия. Этот способ распространения идей и взглядов широко используется западной пропагандой. Один из актуальных примеров навязывания образа врага в лице России – разработанная американской компанией Infinity Ward серия игр «Call of Duty» (в выпуске от 2023 г. «Call of Duty: Modern Warfare 3» вымышленные «российские» ультраправые войска оккупируют Нью-Йорк) [25]. Однако создание виртуальных игровых пространств на базе метавселенных дешевле и проще, чем выпуск полноценных игр. Пользователи, создающие свои игровые локации, могут использовать пропагандистские ролики, символику запрещенных организаций, создавать определенное

---

[1] На уровне физиологических реакций интенсивность эмоций, полученных в виртуальном пространстве, соизмерима с эмоциями, полученными в реальном мире. В ряде исследований сообщается, что виртуальная реальность лучше стимулировала эмпатию и чувство вовлеченности, чем при восприятии 2D-информации, что побудило зрителей к действиям в реальной жизни (в случае, описанном в исследовании, речь шла об оказании финансовой помощи) [24].

[2] Исходя из изученных исследований, а также современных тенденций ведения информационно-психологических операций, можно утверждать, что зачастую в основе воздействия, особенно в случае дезинформации, лежит эмоциональное манипулирование.

ролевое взаимодействие, направленное на разжигание ненависти или внедрение запрещенных идей.

Игровое взаимодействие подразумевает не только шутеры от первого лица, но и так называемые ролевые игры (англ. Role Play), где пользователи, воплощенные в своих аватарах, могут осуществлять и сексуальное взаимодействие. В частности, в сервисах VRChat и Second Life широко распространены такие активности и девиации, как однополые отношения, фембои, фурри, трансгендеры и зоофилы. До недавнего времени[1] в Second Life было разрешено использование детских аватаров. В настоящее время в сервисе происходит ужесточение политики использования изображений несовершеннолетних, однако ее эффективность вызывает сомнения с учетом возможности использования приватных локаций, слабой модерации контента, а также случаями доступа к контенту для взрослых пользователей с учетной записью несовершеннолетних.

Даже возможность создания платформ для обучения может применяться в целях формирования искаженного исторического контекста. На базе ряда метавселенных уже созданы платформы для проведения образовательных программ с использованием VR, которые продвигают западную трактовку событий. Так, например, на мемориалах Second Life, посвященных жертвам первой и второй мировых войн, не упоминаются русские и советские солдаты.

Выводы. В статье представлены наиболее очевидные потенциальные угрозы метавселенных в информационно-психологической сфере, а также описаны некоторые способы воздействия на аудиторию виртуальных пространств. Стоит отметить, что такие способы не являются принципиально новыми, все они известны и реализуются западной пропагандой в классических средствах массовой информации и коммуникации. К ним относятся: убеждение, разъяснение, обсуждение, информирование, распространение слухов, дезинформация и пр. Однако в метавселенных их эффективность усиливается за счет иммерсивного повествования, большего погружения и усиления эмоционального воздействия, игрового взаимодействия и использования платформ для обучения, что улучшает восприятие информации.

Сложившееся положение с распространением деструктивного контента усугубляется сложностями с его обнаружением и модерацией, в частности, основное общение происходит посредствам голоса, что подразуме-

---

[1] В связи с участившимися жалобами Second Life внесла изменения в политику, касающуюся детских аватаров. Детским аватарам будет запрещено появляться в регионах с рейтингом «для взрослых», участвовать в любых игровых событиях или находиться в локациях, подразумевающих эпизоды 18+. Создатели детских аватаров обязаны покрывать кожу аватаров непрозрачным плотным слоем, отличающимся от тона кожи, который не может быть стерт или удален, а также не должен выглядеть вызывающим. Также добавлен ещё ряд правил, защищающих детские аватары от неподобающего контента в виртуальном мире [26].

вает необходимость его перевода в текст и последующий анализ, а это требует дополнительных вычислительных мощностей. Кроме того, выявлено, что в ряде сервисов, например, в Second Life возрастная маркировка контента имеет условный характер, т.к. пользователь с учетной записью несовершеннолетнего имеет к нему полный доступ.

Для противодействия выявленным угрозам необходимо разработать способы и методы оперативного обнаружения деструктивного и запрещенного на территории РФ контента с учетом описанных выше особенностей распространения информации в метавселенных, а в последующем – также выработать меры противодействия распространению подобной информации, в особенности среди социально незрелых и уязвимых слоев общества.

Литература

1. Anthony Turner. Generation Z: Technology and social interest. // The Journal of Individual Psychology, Volume 71, Number 2, Summer 2015, pp. 103-113.
2. The metaverse challenges and regulatory issues [Электронный ресурс]. – URL: https://www.sciencespo.fr/public/sites/sciencespo.fr.public/files/Metaverse-Group-report-final-draft-June-12-1.pdf (дата обращения 20.01.2023).
3. How Media Use Can Affect Kids [Электронный ресурс]. – URL: https://kidshealth.org/en/parents/tv-affects-child.html (дата обращения 20.01.2023).
4. Porn survey reveals extent of UK teenagers' viewing habits [Электронный ресурс]. – URL: https://www.theguardian.com/culture/2020/jan/31/porn-survey-uk-teenagers-viewing-habits-bbfc (дата обращения 20.01.2023).
5. What’s a Furry? [Электронный ресурс]. – URL: https://furscience.com/whats-a-furry/ (дата обращения 21.06.2024).
6. Львова-Белова прокомментировала распространение движения «фурри» [Электронный ресурс]. – URL: https://ria.ru/20240607/lvova-belova-1951242858.html (дата обращения 21.06.2024).
7. The risks of earlier puberty [Электронный ресурс]. – URL: https://www.apa.org/monitor/2016/03/puberty (дата обращения 20.01.2023).
8. Camilla Eckert-Lind, Alexander S. Busch, Jørgen H. Petersen, Frank M. Biro, Gary Butler, Elvira V. Bräuner, Anders Juul, Worldwide Secular Trends in Age at Pubertal Onset Assessed by Breast Development Among Girls, JAMA Pediatr, 2020 Apr; 174(4): e195881, doi: 10.1001/jamapediatrics.2019.5881, PMCID: PMC7042934, PMID: 32040143.
9. Rises in Early Puberty May Have Environmental Roots [Электронный ресурс]. – URL: https://www.scientificamerican.com/article/rises-in-early-puberty-may-have-environmental-roots/ (дата обращения 20.01.2023).
10. New Research Shows How Evolution Explains Age Of Puberty [Электронный ресурс]. – URL: https://www.sciencedaily.com/releases/2005/12/051201022811.htm (дата обращения 20.01.2023).
11. The health risks of maturing early [Электронный ресурс]. – URL: https://www.bbc.com/future/article/20180611-the-health-risks-of-girls-maturing-early (дата обращения 20.01.2023).
12. The end of the Flynn effect?: A study of secular trends in mean intelligence test scores of Norwegian conscripts during half a century [Электронный ресурс]. – URL:

https://www.sciencedirect.com/science/article/abs/pii/S0160289604000522?via%3Dihub (дата обращения 20.01.2023).

13. Lisa Trahan, Karla K. Stuebing, Merril K. Hiscock, Jack M. Fletcher The Flynn Effect: A Meta-analysis, Psychol Bull. 2014 Sep; 140(5): 1332–1360, doi: 10.1037/a0037173, PMCID: PMC4152423, NIHMSID: NIHMS599844, PMID: 24979188.

14. British teenagers have lower IQs than their counterparts did 30 eyers ago [Электронный ресурс]. – URL: https://www.telegraph.co.uk/education/educationnews/4548943/British-teenagers-have-lower-IQs-than-their-counterparts-did-30-years-ago.html (дата обращения 20.01.2023).

15. Bratsberg B, Rogeberg O. Flynn effect and its reversal are both environmentally caused. Proc Natl Acad Sci U S A. 2018 Jun 26;115(26):6674-6678. doi: 10.1073/pnas.1718793115. Epub 2018 Jun 11. PMID: 29891660; PMCID: PMC6042097.

16. Malevolent Creativity & the Metaverse: How the immersive properties of the metaverse may facilitate the spread of a mass shooter's culture [Электронный ресурс]. – URL: https://owogame.com/owo-skin-acm/ (дата обращения 21.06.2024).

17. How Video Games Could Facilitate Radicalization Processes [Электронный ресурс]. – URL: https://www.rcc.int/swp/news/278/how-video-games-couldfacilitate (дата обращения 15.05.2023).

18. United Nations Office counter-terrorism - Examining the Intersection Between Gaming and Violent Extremism [Электронный ресурс]. – URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf (дата обращения 15.05.2023).

19. Rising Scores on Intelligence Tests [Электронный ресурс]. – URL: https://journals.lib.sfu.ca/index.php/jicw/article/view/5038 (дата обращения 11.05.2023).

20. Как я участвовала в оргиях в Роблоксе и другие байки из нижнего метаверса [Электронный ресурс]. – URL: https://dtf.ru/games/1854662-kak-ya-uchastvovala-v-orgiyah-v-roblokse-i-drugie-bayki-iz-nizhnego-metaversa (дата обращения 31.05.2023).

21. Assassin's Creed Mirage Edition [Электронный ресурс]. – URL: https://owogame.com/owo-skin-acm/ (дата обращения 21.06.2024).

22. Баранов Е.Г. Информационно-психологическое воздействие: сущность и психологическое содержание. // Национальный психологический журнал 2017. № 1. с.25-31. doi: 10.11621/npj.2017.0103.

23. Касюк А.Я. Информационно-психологическое воздействие в информационном противоборстве. //Вестник Московского государственного лингвистического университета. Общественные науки. Выпуск 1 (842) / 2021. с. 22-34. doi: 10.52070/2500-347X_2021_1_842_22.

24. Manipulation und Desinformation im Metaverse [Электронный ресурс]. – URL: https://owogame.com/owo-skin-acm/ (дата обращения 21.06.2024).

25. Call of Duty: Modern Warfare 3: Story [Электронный ресурс]. – URL: https://www.interpol.int/content/download/18440/file/INTERPOL%20Tech%20Assessment-%20Metaverse.pdf (дата обращения 11.05.2023).

26. SECOND LIFE - CHILD AVATAR POLICY UPDATE, INVESTIGATION OUTCOME & COMMUNITY ROUND TABLE [Электронный ресурс]. – URL: https://www.youtube.com/watch?v=znjqigC1p1A&list=PL74x3jdmaEIdhzG51eo-aKGgA0AM3dIYP&index=2 (дата обращения 21.06.2024).

Еськов Александр Васильевич,
доктор технических наук, профессор
начальник кафедры
информационной безопасности
Краснодарского университета МВД России

ВОВЛЕЧЕНИЕ ПОДРОСТКОВ В ТЕРРОРИСТИЧЕСКУЮ И ЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ В СЕТИ ИНТЕРНЕТ

Терроризм становится основной угрозой для человечества и его безопасности, и его предотвращение должно быть общей задачей международного сообщества. Он несет угрозу национальной безопасности России и противостоять ему в полном объеме способно государство, общество и гражданин. Здесь важно противостоять привлечению молодого поколения в террористическую деятельность, ввиду того, что существует опасность деформирования понимания общества, себя в нём, вследствие внедрения в сознание экстремистских идей. Наиболее удобной средой общения для этого вербовщики выбирают всеми известную сеть Интернет, в которой молодое поколение проводит достаточно много времени.

Доступность Интернета, его популярность дает возможность не только управлять мышлением отдельных людей или групп, но также влиять во многих ситуациях на основной потенциал российского общества – национальный менталитет, культуру, психологическое состояние граждан. Подростки – наиболее подходящий слой населения для этого. Неустойчивая психика, отсутствие критического подхода к получаемой информации позволяют воспринимать сообщения, «мультики» или компьютерные игры о «добрых» террористах, борцов за правое дело как о положительных героях. Наградой за это могут выступать электронные деньги, очки, фишки, бонусы, необходимые для получения и хранения.

Некоторые факторы и социальные явления, способствующие вовлечению подростков в экстремистскую деятельность в Интернете:

– социальная отчужденность, усиление эгоизма, депрессивных настроений в рядах молодежи;

– уменьшение защищенности особенно важных интересов подростка;

– постепенное вовлечение несовершеннолетних в криминальную сферу;

– упадок моральных устоев, обесценивание традиций, культуры и истории России, а также таких понятий как долг и честь;

– усиление пропаганды террористических идей с применением современных коммуникационных средств.

Наиболее подверженными такому риску являются следующие группы подростков:

- находящиеся или склонные депрессии;
- со слабой душевной организацией;

- неуверенные в себе;
- имеющие искажённое представление о мире;
- легко поддающиеся влиянию дети.

Многие вербовщики общаются с поддельных аккаунтов, однако их довольно просто вычислить. На таких страницах в социальных сетях могут отсутствовать настоящие фотографии либо они взяты с чьих-то страниц (это можно проверить, если сделать поиск изображения в какой-нибудь поисковой системе). Почти все подростки, так или иначе, стараются скрывать личную жизнь, особенно от своих родителей. Однако при отсутствии нормального общения такая скрытность становится паранойей – появляются браузеры, предназначенные для доступа к незаконным сайтам, переписки продолжаются в мессенджерах, доступ к которым имеет только сам подросток; часто производится смена паролей, появляются личные ложные аккаунты.

Подросток, который попал под воздействие преступников, может не выдавать себя подписками на подозрительные группы, хотя косвенные признаки все же можно обнаружить. Главный из них – очень тесное, зацикленное общение с онлайн-другом, заменяющее общение со сверстниками в реальности, также отсутствие реальных встреч с этим человеком, попытки скрытия общения и тем разговоров. При этом попытки родителей отграничить своих детей от Интернета заканчиваются ссорами и агрессией детей. Хотя этот факт может говорить не только о привлечении подростка к террористической деятельности, но и о его психологических проблемах.

Терроризм в сети в отношении подростков может повлечь за собой следующие негативные последствия:

получение необходимой информации путем психологического воздействия злоумышленниками;

вовлечение подростков в незаконные мероприятия, а также массовые беспорядки;

подстрекательство и пособничество несовершеннолетних к совершению преступлений;

массовый психоз подростков и доведение их до самоубийства;

запугивание, дезинформация, разрушение эмоциональных устоев подростка;

внедряясь в доверие детей, злоумышленники выманивают деньги своими неправомерными действиями.

С учетом важности Интернета как самого используемого экстремистами канала распространения данных и эффективного метода противостояния им, в некоторых регионах Российской Федерации получен достаточно большой положительный опыт действий в сети. Например, в 2012 году по инициативе студенческих объединений и молодых ученых главных вузов страны в целях противостояния экстремистской и террористической деятельности в Интернете были спроектированы специально предназначенные для этого интернет-ресурсы.

Также следует отметить положительный опыт обсуждения актуальных проблем, связанных с идеологией экстремизма и терроризма, с применением возможностей интернета в виде онлайн-семинаров. Возможности для увеличения объем участников при этом почти не ограничены и зависят только от начальной осведомленности его будущих участников. Как говорят специалисты в области противодействия экстремизму и терроризму в киберпространстве, молодежи следует шире использовать возможности их социальных сетей для проведения на регулярной основе активных пропагандистских акций. Для этого нужен корректный, уважительный формат отношений с наиболее активными пользователями, которые инициативно готовы содействовать государству и населению в противостоянии привлечения подростков к терроризму.

Кроме того обезопасить своих детей от ненужной, негативной информации можно при помощи специального плагина для браузера «Родительский контроль» или одноименной системы, встроенной в антивирус. Такое программное обеспечение обладает следующими функциями:

блокирует доступ к сомнительным сайтам и их содержанию;

помогает управлять доступом к играм и нежелательным приложениям;

позволяет отслеживать время использования каждого устройства;

предоставляет отчеты о публикациях и подписках ребенка в социальных сетях;

предоставляет советы специалистов по поводу активности ребенка в сети.

На сегодняшний день молодежь в Интернете – один из основных, наиболее уязвимых объектов агитационно-пропагандистских целей террористов и экстремистов, имеющих цель увеличения круга своих последователей, посредников и пособников. Эффективность профилактики всей системы терроризма в Интернете по большей степени определяется тем, насколько она активно противостоит распространению этой идеологии среди подростков. Высокий результат в этой работе невозможен без активного участия в ней структур гражданского общества.

Литература

1. Шишина Е.А. Использование сети Интернет в целях вовлечения в экстремистскую деятельность // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2022. – Т. 8 (74). № 3. – С. 402-407.

2. Осипенко А.Л., Соловьев В.С. Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий // Общество и право. – 2019. № 3 (69). – С. 23-31.

Ефимова Юлия Сергеевна,
преподаватель
Краснодарского университета МВД России

Никоненко Елизавета Вадимовна,
курсант Краснодарского университета МВД России

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ИДЕНТИФИКАЦИИ И БЛОКИРОВКИ ЭКСТРЕМИСТСКОГО КОНТЕНТА В СОЦИАЛЬНЫХ СЕТЯХ

Искусственный интеллект в настоящий момент является наиболее часто встречающейся технологией, обсуждаемой научным сообществом в контексте использования в качестве вспомогательного инструмента для осуществления множественных манипуляций: анализа больших данных, применения в различных сферах общественной жизни: в медицине, экономике, логистике и иных, где требуется значительное количество временных и человеческих ресурсов. Автоматизация многих процессов обусловила стремительное распространение нейросетей.

Использование современных достижений науки и техники является одним из принципов деятельности полиции, утвержденных Федеральным законом «О полиции». Очевидно, что вопрос использования искусственного интеллекта является важным не только в контексте автоматизации вычислительных процессов обработки информации, но и в построении логических связей и принятии некоторых управленческих решений.

Использование искусственного интеллекта в деятельности полиции обсуждается в Министерстве внутренних дел регулярно, поскольку правоохранительные органы заинтересованы в увеличении показателей раскрываемости различных видов преступности, в том числе осуществляемых в киберпространстве или с использованием информационно-коммуникационных технологий и других технологических решений.

В 2024 г. Министерство внутренних дел собирается провести научно-исследовательскую работу (НИР) и подготовить датасеты для обучения и тестирования нейросетевых моделей, а в 2025 г. разработать две системы на базе ИИ «Клон» и «Конъюнктура». «Клон» позволит выявлять факты подделки видеоизображений в интересах правоохранительной деятельности, «Конъюнктура» должна прогнозировать негативные события и чрезвычайные ситуации и моделировать сценарии реагирования на них.

Такие мероприятия включены в план по внедрению технологий ИИ в деятельность органов внутренних дел РФ на 2023–2025 гг. План утвержден заместителем министра внутренних дел Виталием Шуликой. «Ведомости»

ознакомились с документом, его подлинность подтвердил сотрудник крупного IT-интегратора, работающего с госзаказами. «Ведомости» направили запрос в МВД России[1].

Источники СМИ сообщили, что подведомственный Роскомнадзору Главный радиочастотный центр (ГРЧЦ) запустил в эксплуатацию интеллектуальную систему отслеживания незаконного контента в интернете «Окулус».

«Информационная система «Окулус» уже запущена и выполняет возложенные на неё задачи в полном объёме: выявляет нарушения законодательства в изображениях и видеоматериалах. В декабре 2022 года система была протестирована, а в январе 2023 г. началась интеграция системы с другими инструментами мониторинга Роскомнадзора», – заявил СМИ представитель ГРЧЦ.

Главная задача системы – это выявление нарушений российского законодательства в изображениях и видеороликах, уточнили в надзорном ведомстве.

«Система распознает изображения и символы, противоправные сцены и действия, анализирует текст в фото- и видеоматериалах. «Окулус» автоматически обнаруживает такие правонарушения, как экстремистская тематика, призывы к массовым незаконным мероприятиям, суициду, наркотический контент, пропаганда ЛГБТ и другие запрещённые действия», – пояснил СМИ представитель ГРЧЦ[2].

Целесообразно применять возможности искусственного интеллекта при предупреждении и проведении расследований преступлений путем сбора, анализа и интерпретации информации, относимой к конкретному совершенному преступлению. Так, использование технологий искусственного интеллекта может существенно упростить задачу для правоохранительных органов по поиску информации о возможных проявлениях экстремистского поведения пользователей в социальных сетях. В современном мире интернет играет важную роль в распространении не только полезной и значимой информации, но и распространению материалов, негативно влияющих на общество, например экстремистских и террористических материалов.

Как сообщает ТАСС, Генеральная прокуратура Российской Федерации постоянно контролирует информацию в интернете, мессенджерах и социальных сетях на предмет наличия противоправного контента.

По состоянию на 25 декабря 2023 года, надзорное ведомство направило в Роскомнадзор более 2000 требований о внесудебном ограничении доступа к информации в интернете. В 2022 году было направлено 1699 таких требований.

---

[1] Кинякина Е. Устинова А. МВД привлечет нейросети к поиску правонарушителей. Ведеомсти, 11 января 2024 г. // Режим доступа: https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei

[2] Роскомнадзор запустил систему автоматического поиска запрещенного контента «Окулус». Ведомости, 13 февраля 2023 // https://www.vedomosti.ru/technology/articles/2023/02/13/962682-roskomnadzor-zapustil-sistemu-poiska-okulus

Как уточнили в Генпрокуратуре, они выявляют онлайн-сервисы, которые предлагают купить поддельные документы или содержат информацию с нарушением законов «О рынке ценных бумаг», «О Центральном банке РФ», «О банках и банковской деятельности». Такие ресурсы могут предлагать вложения в ценные бумаги или получение кредитных услуг в обход действующего законодательства, включая финансовые пирамиды.

За 2023 год надзорное ведомство направило в Роскомнадзор 306 требований об ограничении доступа к 41 798 интернет-ресурсам, включая сайты, страницы в социальных сетях, приложения и другие платформы, содержащие противоправный контент[1].

Одним из основных типов применяемых искусственным интеллектом технологий по анализу текстовых материалов в сети Интернет является обработка естественного языка. При обучении анализу текста нейросеть обучается в процессе обработки больших объемов текстов, содержащих как информацию, запрещенную для распространения и публикации, так и отвлеченные от преступной деятельности материалы. В процессе подобного целевого обучения искусственный интеллект учится распознавать ключевые слова, фразы и речевые обороты, прямо или косвенно указывающие на наличие экстремистских материалов. Семантический и эмоциональный анализ текста, проводимый искусственным интеллектом, используется для определения эмоциональной окраски и смыслового содержания текста. Подобный анализ предназначен для выявления эмоционально окрашенных слов и идентификации текстов различной смысловой и содержательной нагрузки, в том числе возможных сведений, представляющих угрозу для общественной безопасности.

Искусственный интеллект обладает способностью анализировать не только текстовый, но и графический контент, такой как различные изображения и видеофрагменты с помощью технологий компьютерного зрения. Алгоритмы компьютерного зрения применяются для распознавания объектов, символов или ситуаций, связанных с различными видами преступлений. Например, нейросеть может идентифицировать различные виды оружия, флаги и символику экстремистских организаций в публикуемых материалах на страницах социальных сетей. Многие разработчики служб модерации и обеспечения безопасности социальных сетей используют подобные технологии с целью предотвращения публикации подобных материалов в качестве превентивных мер по безопасности.

Использование искусственного интеллекта для выявления экстремистских материалов в интернете является мощным инструментом, позволяющим обеспечить безопасность пользователей в цифровом пространстве со-

---

[1] Матвеев Д.Искусственный интеллект займется блокировкой экстремистского контента в России. Телеспутник, январь 2023 // Режим доступа: https://telesputnik.ru/materials/gov/news/iskusstvennyy-intellekt-zaymetsya-blokirovkoy-ekstremistskogo-kontenta-v-rossii

циальных сетей и Интернета. Несмотря на возможные технические трудности, такие как ложные срабатывания алгоритмов безопасности и необходимости постоянного обновления базы знаний, используемой искусственным интеллектом, данная технология продолжает развиваться, применяясь в новых сферах общественной жизни. При условии эффективного использования инструментов и технологий, соблюдении стандартов безопасности по использованию средств автоматизации искусственный интеллект и нейросети имеют потенциал по повышению безопасности пользователей в Интернете.

Литература

1. Кинякина Е. Устинова А. МВД привлечет нейросети к поиску правонарушителей. Ведеомсти, 11 января 2024 г. // Режим доступа: https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei

2. Матвеев Д. Искусственный интеллект займется блокировкой экстремистского контента в России. Телеспутник, январь 2023 // Режим доступа: https://telesputnik.ru/materials/gov/news/iskusstvennyy-intellekt-zaymetsya-blokirovkoy-ekstremistskogo-kontenta-v-rossii

3. Роскомнадзор запустил систему автоматического поиска запрещенного контента «Окулус». Ведомости, 13 февраля 2023 // https://www.vedomosti.ru/technology/ articles/2023/02/13/962682-roskomnadzor-zapustil-sistemu-poiska-okulus

Здун Тимофей Алексеевич,
старший научный сотрудник
Краснодарского высшего военного училища
имени генерала армии С.М.Штеменко

ВОПРОСЫ УЧЕТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ОГРАНИЧЕННОГО ДОСТУПА

Цифровые технологии постепенно совершенствуются и интегрируются во все сферы жизни, что приводит к значительным изменениям во всех сферах жизни общества. Эти изменения в свою очередь стимулируют развитие науки и техники, что проявляется в использовании новых методов для повышения эффективности в том числе и государственного управления. В настоящее время наблюдается активное и инновационное применение веб-технологий для модернизации различных процессов с целью улучшения их результативности. Например, концепция электронного правительства предполагает использование систем электронного документооборота и автоматизации управления для повышения прозрачности и ответственности во взаимоотношениях между правительством и гражданами. Однако переход к таким системам в государственных и частных структурах сталкивается с проблемами, информационной безопасности. Поэтому необходимо проанализировать свойства электронных документов с технической точки зрения и разработать методы их безопасного обращения, в частности, решить задачи учета, аутентификации, копирования и хранения документов ограниченного доступа.

В ходе предварительного анализа возможностей современный систем электронного документооборота были рассмотрены следующие системы и оценены их преимущества и недостатки: Битрикс24, СБИС, Контур.Диадок, Microsoft SharePoint, DocuWare, Laserfiche, M-Files, OpenText Content Suite, 1С:Документооборот.

Системы поддерживают возможности многофакторной аутентификации, шифрования данных как при передаче, так и при их хранении, ограничение прав пользователей на просмотр, редактирование, копирование и печать документов, контроль версий, ведение логов, интеграция с DLP и прочие инструменты безопасности.

В то же время имеются ряд уязвимостей в данных системах, такие как:

уязвимости в плагинах и расширениях;

возможности внутреннего злоупотребления доступом;

риски при передаче данных через интернет;

риски утечки данных при интеграции с другими системами;

риски утечки данных при неправильной конфигурации системы;

риски утечек данных при их передаче во взаимодействующие организации.

Поэтому системы электронного документооборота не решают в полной мере задачи обеспечения безопасности электронных документов ограниченного доступа, т.к. для их решения в том числе необходима глубокая интеграция формата представления ЭД с реализуемыми возможностями СЭД. В данный момент СЭД имеют возможность делать записи во внутренних базах данных о реквизитах документа и его принадлежности, без изменения внутреннего содержимого документа, его метаданных [9], т.е. учетные данные присвоены электронному документу условно. Сам файл остается неучтенным, и возможно создание неограниченного числа его копий, которые могут бесконтрольно распространяться как внутри системы, так и за ее пределами, что противоречит основным принципам работы с документами ограниченного доступа [1, 8].

Анализ существующих на настоящий момент нормативных документов в данной области показал, что отсутствует определение порядка представления электронного документа в конкретном формате, который позволял бы различать оригинал и копии. Также существующая нормативно-правовая база не регламентирует технические вопросы создания электронных документов, их движения и учета [2, 3, 4, 5, 6, 7].

Для решения указанных проблем предлагается стандартизировать формат представления электронного документа и разработать систему маркировки и учета электронных документов ограниченного доступа.

В качестве нового формата электронного документа предлагается модель электронного документа, имеющего следующие функциональные особенности, отличающие его от электронных документов существующих форматов, таких как pdf, odt, docx:

1. Расширенные поля метаданных с возможностью записи логов проводимых операций с документом. Метаданные разделяются на открытые и закрытые. Открытые включают в себя информацию о политике общего доступа к документу. Закрытые метаданные содержат следующую информацию: ограничительные пометки документа, владелец документа, учетный номер документа, проведенные операциях с документом и/или контентом документа, имеющиеся подписи документа, историю владения документа, историю его движения.

2. Активные свойства документа, позволяющие ему:

определять безопасность окружающей его среды;

самоуничтожаться в случае попытки доступа вне безопасной среды;

оповещать о своем местоположении при попытке несанкционированного доступа.

Под безопасной средой в данном случае понимается авторизованная автоматизированная систему (отдельные автоматизированные рабочие места (АРМ) с настроенными в соответствии с требованиями руководящих документов политиками безопасности и реализованной системой маркировки и учета электронных документов.

Формально активный электронный документ можно представить в кортежном виде:

$$ad = (C, A, M) \quad (1)$$

где ad – активный электронный документ; C – content, основное содержимое документа; A – модуль активных свойств документа, представленный в виде множества атрибутов безопасности; M – расширенные метаданные, включающие в себя: R – сведения о налагаемых ограничениях, H – сведения о владельце, N – учетный номер, S – подписи, L_D – данные о проводимых с документом операциях, G – политика общего доступа (сведения о допущенных пользователях).

Авторизацию системы (отдельного рабочего места) предлагается производить с помощью присвоению системе (АРМ) идентификационного номера с записью в иерархически распределенную базу данных, а также защиту указанного механизма криптографическими средствами.

Также предлагается ввести понятие формы электронного документа – совокупность данных, которые обрабатываются в системе до их подписания уполномоченными лицами. После подписания форма уничтожается, системой создается электронный документ с соответствующими реквизитами.

При этом подобные документы не могут существовать сами по себе, необходима система, которая будет отвечать за весь их жизненный цикл.

Следующим важным шагом перехода к электронному документообороту с использованием информации ограниченного доступа является разработка системы маркировки и учета электронных документов.

Указанная система должна обеспечивать выполнение следующих операций:

учет выданных пользователям электронных документов (форм);

учет подписанных электронных документов;

обеспечение целостности и неотречимости электронных документов (защита содержимого и метаданных с помощью криптографических методов);

защита содержимого электронных документов с использованием криптографических методов;

обеспечение авторизованного доступа к содержимому электронных документов (открытие/закрытие сессий работы с электронными документами в соответствии с наложенными ограничениями и политикой общего доступа);

ведение логов операций с электронными документами;

обеспечение защищенных криптографическими методами каналов общения между системой, пользователем и документом.

Таким образом, система в общем виде будет представлять собой совокупность следующих множеств:

$D_R = (r_i \mid i = \overline{1,nR})$ – база данных возможных ограничений доступа, накладываемых на документ, nR – общее число возможных ограничений;

$U = (u_i \mid i = \overline{1,nU})$ – множество пользователей (групп пользователей) с указанием их прав, nU – общее число пользователей;

$D_F = (f_i \mid i = \overline{1,nF})$ – база данных выданных форм, nF – общее число выданных форм, f_i – последняя выданная форма;

$O = (o_i \mid i = \overline{1,nO})$ – множество возможных операций, проводимых с документами, nO – общее число операций;

$I = (i_q \mid q = \overline{1,nI})$ – множество возможных воздействий на документ, nI – общее число воздействий;

$D_L = (l_i \mid i = \overline{1,nL})$ – база данных логов проводимых операций, nL – общее число записей, l_i – последняя запись в базе данных;

$D_S = (ad_i \mid i = \overline{1,nAD})$ – база данных подписанных документов (учет), nAD – общее число документов в базе, i – учетный номер документа.

Для возможности выполнения поставленных ранее условий необходимо ввести также следующий элемент системы:

$A = (a_i \mid i = \overline{1,nA})$ – модуль аутентификации системы с атрибутами безопасности, nA – общее число атрибутов.

Подводя итог, имеется возможность представить математическую модель системы маркировки и учета электронных документов (СМУ) в кортежном виде:

$$MAS = (A, D_R, D_F, D_S, D_L, U, O, I) \quad (2)$$

где MAS – СМУ, а остальные обозначения введены ранее.

Операция над документом – это целенаправленное воздействие пользователя на документ, включающее изменение одной или нескольких составляющих документа (контент, метаданные).

Операция над документом прежде всего начинается с определения возможности обработки документа ad_0 в системе MAS, т.е. определения безопасности окружения документа. Также, перед проведение операции необходимо удостоверится, что пользователь u имеет права доступа к содержимому C_0 документа ad_0, а также имеет достаточно прав на проведение конкретной операции o с документом (осуществить воздействия i на составляющие документа).

Таким образом общий вид операции можно представить как:

$$o : (ad_0, rreqd) \rightarrow rresd > 0 \rightarrow (ad_0(C_0, A_0, R_0, H_0, N_0, G_0, L_{D0}), u, i, rrequ)$$
$$\rightarrow rresu > 0 \rightarrow (ad_1(C_1, A_0, R_1, H_1, N_1, G_1, L_{D1}), l_D, l_{MAS}) \quad (3)$$

при ограничениях:

документ будет обрабатываться в системе $(rresd > 0)$, если атрибуты безопасности документа $A(ad_0)$ меньше или равны атрибутам безопасности системы A(MAS):

$$A(ad_0) \le A(MAS) \quad (4)$$

пользователю разрешено выполнить операцию с документом $(rresu > 0)$, если права пользователя больше или равны установленным на документ и операцию ограничениям (мандатное и дискреционное разграничение доступа) и пользователь входит в число допущенных к документу (G):

$$r(u) \geq r(ad) \cup r(i) \quad (5)$$

$$u \in G_0(ad_0) \quad (6)$$

Где ad_0 – исходный документ; u – пользователь, производящий операции с документом; i – воздействие пользователя на документ; rrequ – запрос пользователя системе на проведение операций с документом; rreqd – запрос документа системе о ее безопасности (возможности обработки данного конкретного документа на данном конкретном АРМ); rresu – ответ системы о правах пользователя; rresd – ответ системы о ее состоянии; ad_1 – документ после произведенных пользователем операций; l – произведенная в запись об операции с документом (l_D – в метаданных документа, l_{MAS} – в базе данных системы маркировки и учета документов); $A(ad_0)$ – множество атрибутов безопасности документа; A(MAS) – множество атрибутов безопасности СМУ; r(u) – права пользователя; r(ad) – ограничения доступа к документу; r(i) – ограничения доступа операции (возникающие вследствие воздействия на документ).

Соотношение описывает общий принцип действий над документами. Однако при разработке системы потребуется конкретизировать и структурировать операции обработки информации на этапе проектирования конкретных систем.

Для примера, операция создания документа o_{cr} (получение пользователем формы документа) – функция добавление новой формы документа f_i во множество D_F, будет представлять собой следующее выражение:

$$o_{cr} : (d_0(R_0, G_0), u, i, rrequ) \rightarrow rresu > 0 \rightarrow (f_i(C_1, A_1, M_1), l_D, l_{MAS}) \quad (7)$$

при ограничениях (5) и (6).

Так как документа на момент начала проведения операции не существует, то проверка безопасности среды (ad_0, rreqd) опускается, а во втором выражении, обозначающем инициацию пользователем операции, ad_0 замещается некоторыми данными d_0, которыми пользователь будет наполнять форму документа. При этом указанные данные имеют некоторые разграничения доступа R_0 и G_0. Форма документа имеет те же свойства, что и документ, за исключение электронных подписей.

В операции копирования документа проверка безопасности среды необходима, и результатом операции будут два идентичных документа. Также требуется проверить полномочия пользователя для выполнения этой операции.

$$o_c : (ad_0, rreqd) \rightarrow rresd > 0 \rightarrow (ad_0, u, i, rrequ) \rightarrow rresu > 0 \rightarrow (ad_0, ad_{0C}, l_D, l_{MAS}) \quad (8)$$

при ограничениях (4), (5), (6),

где ad_{0C} – копия исходного документа ad_0.

Представив систему и общий вид операций в формальном виде можно выделить отличия от существующих систем электронного документооборота:

1. Обязательный запрос документа системе о ее безопасности rreqd: без положительного ответа дальнейшая работа с документом невозможна. Вне системы этот запрос предотвратит утечки информации, поскольку предлагается внедрить активные свойства в саму структуру документа. В настоящий момент, даже в случае использование в системе специального программного обеспечения, обеспечивающего мандатное и дискреционное разграничение доступа, эти ограничения игнорируются при открытии документа за пределами системы.

2. Обязательный и расширенный запрос пользователя системе на выполнение операций с документом rrequ: пользователь должен быть авторизован, иметь права доступа к содержимому документа, иметь права на проведение операций с документом.

Современные системы электронного документооборота не предлагают решений по защите документов при их передаче за пределы организации. Использование активного документа в сочетании с системой маркировки и учета электронных документов позволит предотвратить внутренние утечки информации за счет полного контроля перемещения документа внутри организации и защитить конфиденциальные данные при их передаче в другие организации. Активный документ, помимо предложенных свойств, может иметь дополнительные функции, например, срок жизни документа, модели взаимодействия с различными пользователями (группами пользователей).

Литература

1. О коммерческой тайне : Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ :принят Государственной думой Федерального собрания Российской Федерации 9 июля 2004 г. :одобрен Советом Федерации Федерального собрания Российской Федерации 15 июля 2004 г. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102088094 [Электронный доступ, дата обращения: 15.04.2024].

2. Об информации, информационных технологиях и о защите информации : Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ :принят Государственной думой Федерального собрания Российской Федерации 8 июля 2006 г. :одобрен Советом Федерации Федерального собрания Российской Федерации 14 июля 2006 г. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264 [Электронный доступ, дата обращения: 15.04.2024].

3. Правила обращения со сведениями, составляющими служебную тайну в области обороны : Постановление Правительства Российской Федерации от 26.11.2021 № 2052. – URL: http://publication.pravo.gov.ru/ Document/View/0001202111290064 [Электронный доступ, дата обращения: 15.04.2024].

4. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования: ГОСТ Р ИСО 15489-1-2007: введ. 01.07.2007. – М.: Стандартинформ, – 2017. – 23 с.

5. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов: ГОСТ Р 7.0.97-2016 :введ. 08.12.2016. – М. : Стандартинформ, – 2017. – 35 с.

6. Информационная технология. Формат Open document для офисных приложений. (OpenDocument) v1.0. ГОСТ Р ИСО/МЭК 26300-2010 :введ. 21.12.2010. – URL: https://docs.cntd.ru/document/1200083207 [Электронный доступ, дата обращения: 15.04.2024].

7. Document management – Portable document format – Part 2: PDF 2.0. International Standard ISO 32000-2:2020 (PDF 2.0) :введ. 12.2020. – URL: https://www.pdfa-inc.org/product/iso-32000-2-pdf-2-0-bundle-sponsored-access [Электронный доступ, дата обращения: 15.04.2024].

8. Конфиденциальное делопроизводство : учеб. пособие / сост. Спичак А.В. – Нижневартовск : НВГУ, – 2020. – 118 с. – URL: https://nvsu.ru/ru/Intellekt/2281/Spichak,_A._V_Konfidencialnoe_deloproizvodstvo1.pdf [Электронный доступ, дата обращения: 15.04.2024].

9. Артемова, И.В. Учет электронных документов в составе библиотечного фонда // Советник в сфере образования. – 2013. – № 4. – С. 62-66.

Карпика Анатолий Григорьевич,
кандидат технических наук, доцент,
доцент кафедры информационного обеспечения ОВД
Ростовского юридического института МВД России

ПРОБЛЕМА РАДИКАЛИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПОСРЕДСТВОМ ОНЛАЙН-ИГР

Противоречие современного мира заключается в том, что появляющиеся новые технологии одновременно несут в себе не только комфорт и удобство для человека, но и нередко содержат новые опасности для него. Действительно, как отмечает С.А. Воронцов, феномен экстремизма уходит вглубь веков, ведь принципом «цель оправдывает средства» отдельные люди руководствовались достаточно давно с исторической точки зрения. И в качестве примера можно привести деятельность секты сикариев в Иудее, находящейся под властью Римской империи в I в. н.э. Члены секты боролись против представителей римской власти, а также с сотрудничающей с ними еврейской знатью. С течением времени данный феномен не оставался неизменным. Одновременно с развитием человечества он преображался с появлением каждого нового элемента научно-технического прогресса.

Относительно текущего состояния дел, согласно официально опубликованным данным Генеральной прокуратуры Российской Федерации, за период с 2018 по 2023 г. (с января по ноябрь) отмечается рост экстремистских преступлений как количественно, так и в долевом выражении от общего количества зарегистрированных преступлений.

Более трех миллиардов человек во всем мире играют в компьютерные игры, которые стали одним из крупнейших секторов развлекательного бизнеса, превзойдя киноиндустрию [1]. Популярные видеоигры являются мощными инструментами для создания социальных связей и развития идентичности, особенно для подростков и молодых людей. Социальные связи и игровые отношения, характерные для игровых пространств, зачастую переносятся из игры в «настоящий» мир в виде встреч и дальнейшей коммуникации в офлайн. Одним из факторов, усилившим эту тенденцию, стала пандемия, во время которой игры стали стандартным способом общения с семьей и друзьями, а также приобретения новых социальных и деловых связей.

Вместе с положительным опытом сохранения традиционных и налаживания новых контактов и связей в период самоизоляции пользователи столкнулись с активизацией различных антиобщественных, преступных и экстремистских групп и сообществ. Известно, что экстремисты используют различные способы для расширения возможностей вести пропаганду своих идей, вербовать новых сторонников, рекрутировать исполнителей террористических и экстремистских акций. Удобным способом для этого стало создание и развитие идентичности игровых пространств для распространения

пропаганды, радикализации участников и даже мобилизации их для террористической деятельности.

В ряде источников описываются акты насилия, совершенные террористами, принадлежащими к онлайн-сообществам, таких как «Буффало», «Шутер Нью-Йорка» и «Крайстчерч», что лишний раз подчеркивают необходимость принятия эффективных мер по борьбе с экстремизмом в играх. Авторы исследований утверждают, что несмотря на прибыльность и популярность игр, приносящих их создателям высокие доходы, понимание необходимости контроля «уровня жесткости» игр и игровых сообществ в интересах устойчивости к экстремистской эксплуатации, остается ограниченным.

Так, во многих игровых студиях не хватает антиэкстремистских ресурсов и опыта, которые крупные социальные сети разработали в последнее десятилетие. Платформы социальных сетей давно используют эффективные инструменты модерации контента в интересах безопасности пользователей, что позволяет вести эффективную борьбу с размещением экстремистских материалов [2]. Отсутствие ресурсов и опыта выявления угроз и экстремистских материалов в игровой индустрии привело к уязвимости в игровых и игровых сообществах, которые экстремисты могут эксплуатировать.

Если говорить об истории этого вопроса, то, например, еще в 2002 году американские неонацистские организации создали и продавали свои собственные игры серии «Белая власть» и модифицированные в этом же ключе популярные игры. В этом же году американский неонацистский лидер Мэтт Хейл заявил, что, если получится повлиять на видеоигры и развлечения, это заставит людей понять, что «мы их друзья и соседи». В 2018 году было обнаружено размещение на игровой платформе Steam сообщества Atomwaffen, также называемого национальным социалистическим орденом, после чего его в конечном итоге запретили.

Опасения по поводу экстремистской эксплуатации цифровых игр и радикализации геймеров в последние годы растет. В сети периодически появляется контент, содержащий демонстрацию, в том числе в прямом эфире, террористических атак с геймифицированными элементами, что позволяет судить о сложности оперативного выявления и блокирования подобных трансляций, что безусловно не снимает ответственности с владельцев этих платформ.

Термин «геймификация» означает эксплуатацию ряда психологических особенностей личности, возникающих при вовлечении пользователей в игру.

1. Использование потребности человека в целостных эмоциональных переживаниях – позволяет обеспечить единство мыслей, чувств и действий, пробудить творческий потенциал, усилить ощущение солидарности и конкуренции.

2. Принцип добровольности – предполагает добровольное участие или создание подобного ощущения у игроков.

3. Вовлеченность – усиливает вовлеченность участников в процесс, используя потребности в достижении успеха и поощрении, познании, общении, влиянии на других.

4. Эксплуатация чувства безопасности – игровая форма снимает напряжение участников и обеспечивает им ощущение защищенности, отсутствия угроз из-за нереальности происходящего в игре.

5. Обеспечение эффекта «размытой ответственности» – участие в игре позволяет человеку снижать контроль и ответственность за свои поступки.

В качестве игровых элементов, применяемых при геймификации, выделяют: уровни (статусы), лидерборды (таблица лидеров/рейтингов), бейджи (виртуальные награды), очки и баллы, шкалу прогресса, продвижение по уровням, дайджесты успеха, интерактивные элементы, виртуальную валюту, виртуальные товары (продукция, которая продается за виртуальные деньги).

Термины «экстремизм» и «радикализация», перекочевавшие в онлайн среду, по своей сути сохранили свое классическое содержание. Экстремизм – это пропаганда крайних взглядов, в том числе вера в то, что успех или выживание внутри группы не могут быть отделены от враждебных действий против внешних групп. Радикализация – это эскалация внутри групп экстремистской ориентации во времени в форме все более негативных новостей о внешней группе, или одобрении все более враждебных или насильственных действий против внешней группы.

Примечательно, что существует несколько различных определений радикализации, и многие ученые и исследователи признают различные, но иногда совпадающие версии «когнитивной радикализации», сосредоточенные на интернализации человека и поддержке насильственных экстремистских убеждений и «поведенческой радикализации», сфокусированной на участие человека в насильственных действиях.

В то время как слова экстремизм и радикализация в реальном мире иногда используются взаимозаменяемо, подобные процессы в играх сопутствуют распространению и нормализации экстремистских идеологий, способствующих процессам радикализации и потенциальной мобилизации к насильственному экстремизму в игровых пространствах. Как выглядит экстремизм в играх?

Экстремистские настроения можно найти повсюду, включая известные цифровые игровые площадки. При этом важно понимать, что они могут принимать различные формы, например, пропаганда, сбор средств, нормализация риторики, экстремистская идеология.

Как выглядит радикализация в играх? Экстремистское содержание создается и распространяется с целью радикализации отдельных лиц и игрового сообщества, что, в свою очередь приводит к нормализации отношения сообщества к экстремистским взглядам, стимулирует набор и мобилизацию участников будущих экстремистских акций. Как может выглядет путь ради-

кализации в играх? Независимо от различий в определениях, эксперты в целом согласны с тем, что люди не становятся радикализированными в течение нескольких дней. Вместо этого существует процесс, который включает в себя комбинацию некоторых базовых индивидуальных уязвимостей или «личных факторов», а также ситуаций и событий, которые «толкают» или «проводят» человека дальше по пути радикализации. Вследствие чего, жертва воздействия может сообщать другим членам сообщества о все более радикальных убеждениях, что в результате может с большей вероятностью привести к участию в акциях, связанных с преследованием других игроков сначала в киберпространстве, а в отдельных случаях и в реальном мире.

Рассматриваемый пример скорее демонстрирует идеальный случай радикализации, так как маловероятно, что человек сообщит, что он радикализируется, так как этот процесс скорее всего будет скрыт от других пользователей. При этом сохраняется вероятность того, что другие игроки могут заметить уже последствия процесса радикализации, например изменение содержания его сообщений в форумах, ненависть в высказываниях и т.п.

Процесс противодействия радикализации пользователей компьютерных игр несомненно требует всестороннего подхода, основанного на принципах разумности и системности. В этой связи хотелось бы выделить следующие аспекты и направления деятельности.

Во-первых, целесообразно разработать механизм верификации возраста игроков. Это позволит более качественно рейтинговать игры и участие в игровых сообществах.

Во-вторых, рассмотреть вопрос о проведении психолого-социального исследования влияния некоторых игр на социальное поведение лиц, имеющих склонность к внушению и совершению правонарушений.

В-третьих, проводить профилактическую работу, направленную на выявление игроков, ведущих деятельность, направленную на радикализацию других игроков и сообществ.

Все эти действия необходимо проводить в тесном контакте с игровыми сервисами и площадками, предоставляющими игровой контент, верифицирующих пользователей и оперирующими игровыми и реальными денежными средствами игроков.

Литература

1. «Использование экстремистами видеоигр – стратегии и тактики» URL: https://home-affairs.ec.europa.eu/system/files/2020-11/ran_cn_conclusion_paper_videogames_15-17092020_en.pdf (дата обращения 04.05.2024).

2. Лемайкина С.В. «Методы обнаружения фальсификации информационного контента» // Юристъ-Правоведъ. 2023. № 3. С. 119-124.

3. Х. Янг «Экстремисты используют видеоигры для набора уязвимой молодежи.» URL: https://theconversation.com/extremists-use-video-games-to-recruit-vulnerable-youth-heres-what-parents-and-gamers-need-to-know-193110 (дата обращения 04.05.2024).

Копцов Сергей Васильевич,
старший преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА КАК СПОСОБ БОРЬБЫ С ЭКСТРЕМИЗМОМ

Экстремизм является сегодня одним из самых опасных видов преступлений. К нему, согласно Федеральному закону от 27 июля 2006 года №148 относятся:

- насильственное изменение основ конституционного строя и нарушение территориальной целостности Российской Федерации (за исключением делимитации, демаркации, редемаркации Государственной границы страны с сопредельными государствами);
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства или неполноценности человека по признаку его социальной, расовой, национальной, религиозной, языковой принадлежности или отношения к религии;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;
- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;
- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединённое с насилием либо угрозой его применения.

Согласно статистике, приводимой главным информационно-аналитическим центром МВД России, за последние годы уровень экстремизма в стране возрос. Так, за 2021 год зарегистрировано 1057 преступлений экстремистского характера на всей территории страны, за 2022 года их количество увеличилось на 48% - зарегистрировано 1566 преступлений данной направленности, за 2023 год по сравнению с 2021 годом зарегистрировано на 27% больше – 1340 преступлений. То есть, после начала Россией Специальной Военной Операции на территории Украины экстремистские организации начали активную работу внутри нашей страны для дестабилизации общественного порядка. Активную деятельность такие организации ведут, используя информационные технологии, к примеру – мессенджеры

«Telegram», «Whatsapp». Так, наиболее ярким примером использования технологий в преступных целях является подстрекательство к беспорядкам в международном аэропорту столицы республики Дагестан – в городе Махачкала. 29 октября 2023 года в телеграмм-канале «Утро Дагестана», оказывая эмоциональное давление на жителей республики, возбуждая национальную ненависть к прибывшим на воздушном транспорте жителям Израиля, что в итоге вылилось в нарушение прав, свобод и законных интересов людей по их религиозному и национальному признаку.

Российская Федерация в целях недопущения подобных случаев сама использует информационные средства для борьбы с экстремизмом.

Согласно стратегии противодействию экстремизму в Российской Федерации до 2025 года одной из задач ставится организация в средствах массовой информации, в сети «Интернет» информационного сопровождения деятельности, направленной на противодействие экстремизму, а также реализация информационного противодействия распространению идеологий экстремизма. Сегодня данная задача решается: на федеральном телевидении ведутся специальные программы, которые направлены на борьбу с данной преступной деятельностью. К таким программам сегодня можно отнести «Стоп Фейк» на телеканале «Россия 24», «Анти Фейк» на телеканале «Первый канал». Благодаря деятельности данных телепрограмм удается объяснять широким массам российского населения способы воздействия различных незаконных организация на мысли людей.

В качестве направления информационной политики России указаны необходимые действия для обеспечения безопасности информационных рубежей государства. К таким действиям можно отнести: проведение мониторинга СМИ и сети «Интернет» для выявления распространения экстремистских материалов, ограничение доступа к таким информационным ресурсам, которые занимаются распространением подобных материалов, создание информационного банка экстремистских материалов, распространение в СМИ и сети «Интернет» социальной рекламы, которая будет направлена на патриотическое воспитание молодых граждан.

Российская Федерация следует данной стратегии. В сети «Интернет» созданы группы, освещающие деятельность органов внутренних дел по борьбе с экстремизмом, такие группы находятся в социальных сетях и мессенджерах, где сегодня проводит своё время значительная часть нашей молодежи. Немало создано групп в мессенджере «Telegram», где освящается деятельность государственных служащих по борьбе с экстремистской преступностью. К таким можно отнести «МВД России», «Следственный комитет РФ» и другие.

Уже созданы банки с информацией о запрещенных организациях К таким можно отнести «Перечень общественных объединений, в отношении которых судом принято вступившее в законнную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным

законом от 25.07.2002 №113-ФЗ «О противодействии экстремистской деятельности», который расположен в открытом доступе на сайте министерства юстиции Российской Федерации.

Сегодня на телевидении уже появляются социальные видеоролики, рассказывающие о традиционных ценностях и недопущении распространения экстремистских идей в обществе. Такая социальная реклама должна появиться и в сети «Интернет», для чего необходимо развивать отечественное программное обеспечение, к примеру различные видеоплатформы, как «Rutube», чтобы повысить интерес общества к данным программным продуктам и в дальнейшем наиболее активно осуществлять агитационную работу по борьбе в том числе с экстремизмом.

Таким образом, Россия ведет активную информационную политику, которая в том числе направлена на борьбу с экстремизмом. В России проводится серьёзная работа по структуризации информации об экстремистских идеологиях, преступлениях и организациях с целью ознакомления широких слоев российского населения с данной информацией, что позволяет уберечь наших граждан от необдуманных поступков. При этом, стоит отметить, что необходимо развивать данное направление, так как, как было сказано вначале, несмотря на довольно высокий уровень уже проделанной работы количество экстремистских преступлений растёт. Именно качественная информационная политика поможет нашей стране справиться с данным типом преступности и даже свети его к минимуму в будущем.

Куминов Михаил Владимирович,
старший преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

НЕКОРРЕКТНО НАСТРОЕННОЕ ТЕЛЕКОММУНИКАЦИОННОЕ ОБОРУДОВАНИЕ В ОРГАНИЗАЦИИ КАК ОДИН ИЗ ПОВОДОВ «ПРИГЛАШЕНИЯ В ГОСТИ» ЗЛОУМЫШЛЕННИКА

В мире существует много типов сетей, предоставляющих пользователям самые разные услуги: звонить по телефону, смотреть передачи по телевизору, слушают радио, причем всё это можно делать как стандартными «устаревшими» способами, так и с помощью новых технологий используя Интернет. Вся интернет сеть подразделяется на глобальные (WAN) и локальные (LAN) сети, которые объединяют людей и эксплуатируемые ими устройства независимо от того, в какой части мира люди находятся. Сейчас мало кто задумывается, как эксплуатируется эти сети, как они работают, как реализована безопасность и что бы было, если бы этих сетей не существовало.

Для реализации указанных сетей используются коммуникационные технологии и телекоммуникационное оборудование[1]. С 90-х годов разница между телекоммуникационным оборудованием и ИТ-аппаратными средствами стала размытой в результате роста Интернета и его возрастающей роли в передаче телекоммуникационных данных. Сейчас можно ещё найти используемые отдельно проложенные провода, специализированных сетей для передачи голоса, видео и компьютерных данных, но, многие до сих пор стремятся получить одновременный доступ к таким сетевым службам с одного устройства по одному физическому каналу.

Вот современные технологии позволяют создать сеть нового типа, предоставляющую несколько видов услуг используя современное телекоммуникационное оборудование с поддержкой возможностей объединения информационных сетей. Появилась возможность смотреть эфирные видеопрограммы на мониторе компьютера, звонить по телефону через Интернет или искать информацию в Интернете, используя экран телевизора. Все это стало возможным благодаря объединению сетей путем грамотного проектирования и настройки телекоммуникационного оборудования.

Настройка телекоммуникационного оборудования – это процесс, в котором принимают участие специально обученные специалисты и инженеры, осуществляющие согласования работы всего оборудования (сетевых устройств) в рамках помещения, здания, фирмы, организации, отдельной территории, региона, страны, эксплуатируемого в одной или в разных сетях.

---

[1] Телекоммуникационное оборудование или коммуникационное оборудование или сетевое оборудование - это тип аппаратного обеспечения, которое используется для телекоммуникаций.

Телекоммуникационным оборудованием может быть следующее:

- коммутационное оборудование (switching equipment) – это маршрутизаторы (router), коммутаторы (switch), концентраторы (hub), ретрансляторы, медиа конверторы и т.д.

- передающее оборудование (transmission equipment) – это различные линии передач (проводные, беспроводные, оптические и спутниковые);

- пользовательское оборудование (customer premises equipment (CPE)) – это оконечные устройства (оборудование) пользователя, локальная сеть (LAN) со своими частными коммутаторами, модемами, стационарными и мобильными телефонными аппаратами и беспроводными устройствами.

В телекоммуникационное оборудование присутствует отдельная категория оборудования (электронных устройств), которые принято считать умными устройствами. В них присутствует программный код (собственная операционная система с набором команд или программными модулями), которым можно управлять локально или дистанционно (переписывать основной программный код, вносить изменения в отдельную память и подключать к любой сети с помощью IP адресации или сетевых технологий).

Производители, выпуская такие умные устройства, для дистанционного доступа прописывали однотипные способы доступа к ним с указанием порядка доступа в инструкции к оборудованию. Благодаря этому в Интернете можно всегда найти эти способы доступов и без труда подключиться к оборудованию выполнив необходимы минимум согласно инструкции (это иметь прямой доступ к оборудованию или в случаи дистанционного подключения иметь возможность обратиться напрямую к сетевому интерфейсу оборудования из доступной компьютерной сети).

Доступ в компьютерной сети можно осуществить двумя способами: или из локальной сети или из глобальной сети. В случаи локальной сети (это когда устройство находится в одноранговой сети и видит все сетевые устройства этой сети), этот способ фактически присутствует всегда, когда оборудование не проходило первичной настройки. В случаи глобальной сети, это кода на устройстве прописали уникальный IP-адрес предоставленный провайдером Интернета и этот адрес становиться доступным всем пользователям Интернета – этот адрес принято называть белым IP-адресом.

После обнаружения умного устройства для осуществления доступа к его программному коду (управляемой оболочке), достаточно ввести логин и пароль по умолчанию согласно типовой инструкции устройства.

Во всех курсах по сетевому администрированию всегда указывается, что нельзя оставлять логин и особенно пароль по умолчанию, что их надо сразу менять при установке и первом запуске. Начиная с 2018 года производителей, выпускаемые такие умные сетевые устройства, стали в законодательном порядке обязывать применять новые требования к выпускаемым

устройствам, у которых возможен доступ не только из локальной сети. В качестве требований были введены два основных правила[1]: а) заводской пароль должен быть уникальным для каждого изготовленного устройства; б) при первом использовании устройство должно требовать смены заводского пароля на «пользовательский» перед тем, как будут доступны все остальные функции.

На отечественных умных устройствах (например фирмы Eltex) применили дополнительный способ защиты: для присвоения необходимого IP-адреса, сетевому администратору необходимо вначале подключить данное устройство локально по отдельному проводу через консольный порт RS-232 к АРМ, осуществить обязательную первоначальную настройку и только после этого у системного администратора появляется возможность дистанционно управлять устройством.

Даже не смотря на такие меры защиты и постоянные напоминания, присутствуют сотрудники, которые игнорируют общепринятые правила по настройке телекоммуникационного оборудования: это на оборудованиях со старыми правилами безопасности оставляют пароли по умолчанию, на новых оборудованиях при смене пароля используют простые пароли или стандартные (к которым они привыкли).

Ещё одной из проблем является халатное отношение руководителей системных администраторов, которые берут на работу сотрудников, не имеющих специальные познания или не прошедших обучающих курсов по данному направлению.

При игнорировании всех этих правил приводит к тому, что в больших организациях при настройке локальной сети часто применяют одноранговую топологию сети, в которой присутствует примерно 1000 пользователей и устройств, территориально сеть расположена в разных зданиях или корпусах отдаленных друг от друга более чем 500 метров. Так как сеть незащищена защищенными VLan каналами, то злоумышленнику достаточно получить доступ к любому АРМ в локальной сети организации и от имени этого АРМ найти незащищенный маршрутизатор или коммутатор, получить к ним доступ. В результате злоумышленник может осуществлять перехват всего сетевого трафика и даже настроит себе выделенный прямой канал для мониторинга и сканирования новых устройств.

Литература

1. Сетевое издание TAdviser. Число кибератак в России и в мире. https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире.

2. Исследовательский центр Positive Research Positive Technologies https://www.ptsecurity.com/ru-ru/research.

3. ServerNews.ru — проект портала 3DNews.ru, посвященный корпоративным и SMB-решениям, а также HPC. https://www.servernews.ru/news.

[1] Статья «Эпоха паролей по умолчанию для серверного и сетевого оборудования уходит в прошлое» с сайта ServerNews.ru — проект портала 3DNews.ru, посвященный корпоративным и SMB-решениям, а также HPC. URL адрес - https://dzen.ru/a/Xr2XuoSoonMUN3Uj

Курносов Денис Александрович,
директор по развитию бизнеса компании «Аросса»,
президент НКО «Ассоциация содействия развитию
цифровых систем «Национальные Смарт Технологии»

БЕЗОПАСНОСТЬ ТЕХНОЛОГИЙ ПРОМЫШЛЕННЫХ СИСТЕМ АВТОМАТИЗАЦИИ – «СЕРАЯ ЗОНА» ИМПОРТОЗАМЕЩЕНИЯ

Несколько хакеров по заказу некой таинственной корпорации создают особенно эффективные программы по взлому защищённой информации. После чего начинается многоступенчатая атака на ключевые элементы инфраструктуры страны. Взламываются правительственные и коммерческие компьютеры по всей территории. Паралич транспорта, отказ коммунальных систем, газоснабжения, энергетики, крах финансовой системы, уничтожение ключевой информации в государственных информационных системах... Именно так развиваются события в американском остросюжетном боевике 2007 года режиссёра Лена Уайзмана «Крепкий орешек 4.0» (англ. Live Free or Die Hard). Если бы не храбрый полицейский Джон Макклейн (в исполнении Брюса Уиллиаса), то выживаемость целой страны была бы под вопросом.

Конечно это был всего лишь режиссёрский вымысел - художественный фильм, в основе сценария которого лежит статья в журнале Wired 1997 года, озаглавленная «Farewell to Arms» («Прощай, оружие»), рассказывающая о новой концепции военных действий. По мнению автора, в новой войне обычное оружие уступит почетное место кибертерроризму и разного рода хакерам. В 1997 году всё это выглядело немного футуристично, и больше было похоже на некую «теорию заговора». Однако прошедшие годы отчетливо показали нам, что не только мошенники, но и террористы понемногу осваивают все новые передовые технологии – «меняют автомат на компьютер и машинный код». И если в 1997 крупные атаки, парализующие жизненно важные системы происходили только в блокбастерах, и их можно было рассматривать сугубо теоретически, то по прошествии лет – это данность, в которой живёт весь мир.

Сегодняшние реалии заставляют нас не только глубоко задуматься над вопросами устойчивости и кибербезопасности функционирования ключевых элементов и систем инфраструктуры Российской Федерации, но и рассматривать такие вопросы как важнейшую задачу обеспечения национальной безопасности. При этом опыт последних лет убедительно показывает нам, что кибертеррористы вполне могут быть на содержании и под защитой не дружественных Российской Федерации государств, стремящихся любыми способами нанести неприемлемый ущерб нашей стране. Кибертерроризм «официально» становится одним из инструментов государственной политики некоторых стран...

В фильме «Крепкий орешек» многоступенчатая атака на разные элементы инфраструктуры страны называлась «Обрушение», в основе которого

почти везде был «нужный код» внутри таких элементов (нужный кибертеррористам). Например, отказ коммунальных систем вполне может быть инициирован путем захвата управления программируемыми логическими контроллерами (далее – ПЛК), которые сегодня почти повсеместно используются на коммунальных объектах, объектах электро- и газоснабжения, а также в системах автоматизации «Умных зданий».

Сегодня сотни тысяч ПЛК используются на производстве и в критической инфраструктуре. И количество таких устройств постоянно растёт. ПЛК управляют и следят за производственными процессами нефтеперерабатывающих заводов, атомных и гидроэлектростанций, магистральных нефте- и газопроводов, включают и выключают системы пожаротушения и дымоудаления аэропортов, ж/д вокзалов, крупных торгово-развлекательных центров, больниц и правительственных зданий.

При этом вызывает серьёзную озабоченность безопасность технологий, которые разработчики ПЛК и систем автоматизации встраивают в свои продукты в энергетике, промышленном производстве, на транспорте, в системах промышленного интернета вещей и т.д. Сегодня большинство таких разработчиков в мире и в России, используют в своих приборах и устройствах готовые OEM-технологий (фреймворки). Это помогает увеличить скорость разработки, снизить её стоимость, улучшить совместимость устройств и т.д.

Однако в результате такого подхода любой, даже максимально «импортозамещённый» ПЛК и система автоматизации получают в свой состав «незаметный» элемент (встроенный машинный код), уязвимости в котором с большой долей вероятности сказываются на безопасности многих, если не всех, продуктов и систем автоматизированного и роботизированного управления технологическим процессом на производстве и в критической инфраструктуре.

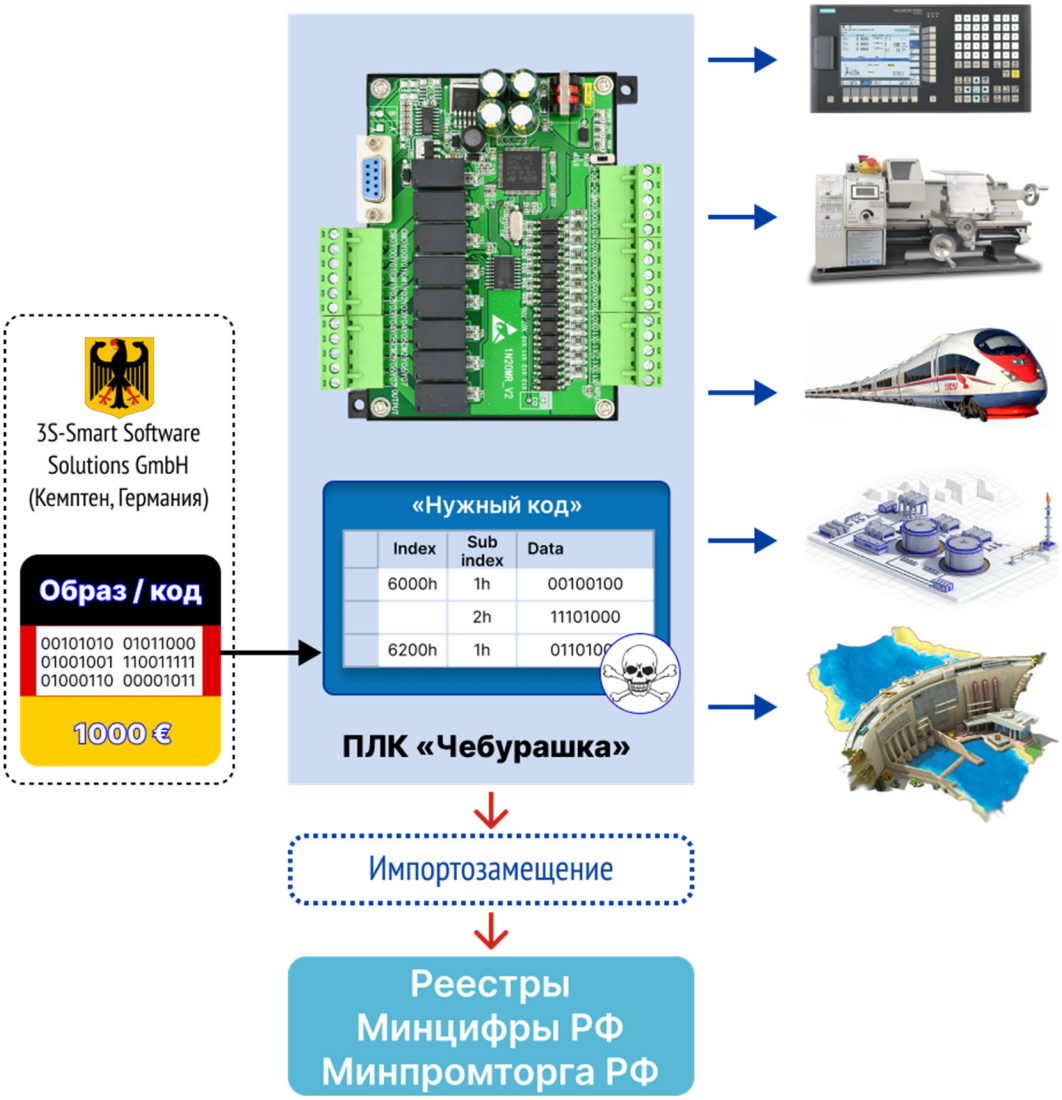


Рис. 1. «Серая зона» импортозамещения.

Учитывая тот факт, что подобные фреймворки являются проприетарными, закрытыми для разработчика ПЛК, технологиями, серьёзно возрастает риск появление в инфраструктуре любой системы «спящего нужного кода», предусмотрительно помещенного туда заранее. На Рисунке 1 приведена схема, которая наглядно иллюстрирует проблему.

Ситуацию следует рассматривать как «серую зону» импортозамещения. С формальной точки зрения импортозамещение уже произошло, и предполагается решить только лишь вопрос замены на российские аналоги импортных (американских, китайских) микроконтроллеров на которых функционируют ПЛК. Выпуск таких «чипов» планируют освоить отечественные предприятия микроэлектроники. Конечно этого недостаточно, ведь в результате внутри российского «чипа» всё равно может оказаться та самая популярная OEM-технология, т.е. тот самый «нужный код»…

Сегодня большое число российских разработчиков и производителей (если не все) включают в состав своих продуктов CODESYS Runtime – популярный во всём мире фреймворк для разработки и выполнения программ

автоматизированного управления технологическим процессом от компании 3S-Smart Software Solutions GmbH (Кемптен, Германия).

За примерами далеко ходить не нужно. Достаточно посмотреть, например, на «ПЛК160 [M02] программируемый контроллер для средних систем» от компании ОВЕН – ведущего российского разработчика и производителя контрольно-измерительных приборов и средств автоматизации для различных отраслей промышленности[1]:

ПЛК160 [M02] программируемый контроллер для средних систем

Для построения распределенных систем управления и диспетчеризации с использованием как проводных, так и беспроводных технологий:

- В системах HVAC
- В сфере ЖКХ (ИТП, ЦТП)
  - АСУ водоканалов
  - линии по дерево- и металлообработке (распил, намотка и т.д.)
- Для управления пищеперерабатывающими и упаковочными аппаратами
- Для управления климатическим оборудованием
- Для автоматизации торгового оборудования
- В сфере производства строительных материалов
- Для управления малыми станками и механизмами

- Простое и удобное программирование в системе CODESYS V.2 через порты USB Device, Ethernet, RS-232 Debug.

USB-драйвер для подключения ПЛК к CODESYS	Windows XP	Windows 7/8/10

Из спецификации специалисты могут понять, что «внутрь» ПЛК160 [M02] заботливо помещён CODESYS Runtime. И таких примеров – множество…

«Исследование безопасности: CODESYS Runtime – фреймворк для управления ПЛК», выполненное Центром реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» в 2019 году, стало одним из первых исследований посвященных вопросам безопасности технологий, входящих в состав продуктов большого количества производителей[2].

Само исследование проводилось методом «черного ящика» - изучалось поведение системы и её реакций на разнообразные внешние воздей-

---

[1] ПЛК160 [M02] программируемый контроллер для средних систем. https://owen.ru/product/plk160

[2] Исследование безопасности: CODESYS Runtime – фреймворк для управления ПЛК. https://ics-cert.kaspersky.ru/publications/reports/2019/09/17/security-research-codesys-runtime-a-plc-control-framework-part-1/

ствия. При этом у исследователей не было никакой информации о «внутреннем устройстве» CODESYS Runtime. Они не имели доступа к исходному коду приложения, а вся информация была получена ими из открытых источников информации и в ходе технического исследования.

В результате исследования было обнаружено 15 уязвимостей. Например, четыре уязвимости в механизме аутентификации приводили к расшифровке передаваемого пароля. Автоматизировав эксплуатацию другой, обнаруженной уязвимости, злоумышленник мог бы долго скрывать свои действия в сети, манипулируя устройствами (т.е. ПЛК) с запущенным CODESYS Runtime и заставляя их отправлять вредоносные пакеты друг другу.

Еще одна уязвимость – это отсутствие песочницы для загружаемой программы. Так фрагменты такой программы представляют собой машинные инструкции, то вместо них злоумышленник вполне мог бы внедрить произвольный, «нужный код», подготовив тем самым, например, газораспределительную станцию к «обрушению» в недалёком будущем…

Выводы

Благодаря широкому распространению и удобству использования CODESYS Runtime на сегодня является «ахиллесовой пятой» любых систем автоматизации и роботизации в Российской Федерации. Это проприетарная технология, исходящая из недружественной юрисдикции, о которой (о составе машинного кода) по сути ничего не известно.

Существующий на сегодня у большинства российских разработчиков и производителей ПЛК подход, заключающейся в применении готовых проприетарных OEM-технологий исходящих из западных юрисдикций является недопустимым и однозначно требует изменений. В первую очередь – внимание государства – необходимо ужесточить требования и регулирование в области импортозамещения продуктов, используемых на производстве и в критической инфраструктуре. В России необходимо создавать свои технологии - фреймворки для разработки и выполнения программ автоматизированного управления технологическим процессом, которые могли бы быть использованы отечественными разработчиками приборов и систем автоматизации для промышленности, энергетики и критической инфраструктуры. Для этого такие технологии должны базироваться на отрытых стандартах и открытом коде.

Лемайкина Светлана Владимировна,
старший преподаватель
кафедры информационного обеспечения ОВД
Ростовского юридического института МВД России

БЛОКЧЕЙН-АНАЛИТИКА ДЛЯ РАССЛЕДОВАНИЯ КРИПТОПРЕСТУПЛЕНИЙ

Блокчейн — особая технология шифрования, хранения и передачи данных, цепочка информационных блоков, формирующих обширную базу (цифровой реестр). Технология блокчейна лежит в основе всех известных криптовалют, но используется не только в финансовом секторе, как могло бы показаться, но и в медицине, недвижимости, управлении, образовании и других отраслях[1]. Неудивительно, что там, где изобилуют экономические возможности, предпринимаются попытки подорвать их с помощью преступлений. Подобно фиатной валюте, криптовалюта использовалась в связи с мошенничеством, программами-вымогателями, отмыванием денег, эксплуатацией детей, финансированием терроризма, уклонением от санкций и торговлей на рынке даркнета.

В 2023 году общий объем крипто-транзакций в размере 24,2 миллиарда долларов был связан с незаконной деятельностью2 Хотя это большая цифра, без контекста она не дает количественной оценки человеческих жертв преступлений, связанных с криптовалютой. Например, одно преступление с криптовалютой – «забой свиней» – это уникальная афера социальной инженерии, в которой мошенники завоевывают доверие жертв с помощью приложений в социальных сетях и текстовых сообщений и обманом заставляют их вкладывать свои деньги на поддельные платформы. Последствия этих мошенничеств были разрушительными, некоторые жертвы потеряли пенсии и пожизненные сбережения, а также душевное спокойствие и уверенность в себе. Издание Forbes сообщало о 52-летнем мужчине из Сан-Франциско, который потерял около миллиона долларов из-за «забоя свиней». В этом случае мошенники выдавали себя за старого коллегу пострадавшего.[3]

Аферы с «забоем свиней» – лишь один из примеров того, как преступники все изощреннее адаптируют свою тактику в последние несколько лет. Сейчас, как никогда, правоохранительные органы должны быть оснащены знаниями и возможностями для борьбы с криптопреступностью.

---

[1] Аналитик блокчейна - кто это такой?https://coinkyt.com/article/analitik-blokchejna-kto-eto-takoj

[2] Тенденции криптопреступности 2024 года: незаконная активность снижается по мере сокращения мошенничества и кражи средств, но рынки программ-вымогателей и даркнета демонстрируют рост https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[3] Криптовалютный скам, называемый «забоем свиней», проник в Apple App Store b Google Play Storehttps://xakep.ru/2023/02/03/pig-butchering-in-app-stores/

Криптовалюты имеют криминальное значение из-за их универсальности как платежного средства, так и инвестиционного инструмента, и ценятся за их анонимность. Криптовалюта часто используется в торговле в даркнете, атаках программ-вымогателей, таких формах взлома, как криптоджекинг, при которых преступники тайно используют вычислительные мощности жертв для майнинга криптовалюты, и отмывании денег. В 2023 году для этой цели было использовано более 22 миллиардов долларов в криптовалюте по всему миру.[1]

Криптовалюта также используется в различных видах мошенничества и была связана с кражами посредством хакерских инцидентов, а также с содействием технологии CSAM (предназначенная для поиска на устройствах материалов о сексуальном насилии над детьми), уклонению от санкций, финансированию терроризма и коммерческим преступлениям - например, при торговле оружием, подделке денег, поддельных документов, продаже наркотиков и лекарств .

Вот некоторые возможности криптовалюты, которые делают ее желательной для криминального использования:

— **Псевдонимность**: Некоторые преступники ошибочно воспринимают криптовалюту как анонимную, хотя на самом деле это псевдоним, потому что криптобиржи обязаны хранить информацию о клиентах в соответствии с правилами «знай своего клиента». Тем не менее, крипто-транзакция в блокчейн-реестре изначально идентифицируется только по публичному адресу, и поиск физического или юридического лица, контролирующего этот адрес, требует определенной работы;

— **Скорость, стоимость и простота использования**: Криптовалютные транзакции, в том числе совершаемые через границы, быстрее и намного дешевле, чем стандартный банковский перевод, вдобавок к тому, что они анонимны;

— **Тактика обмана**: Преступники, пытающиеся отмыть средства, часто прибегают к криптомикшерам, сервисам, которые скрывают происхождение и назначение криптовалютных транзакций;

— **Потенциальная отдача от инвестиций**: Опять же, криптовалюта представляет привлекательную инвестиционную возможность для некоторых преступников, тем более что она не привязана к традиционным финансовым рынкам.

Хотя блокчейн прозрачен, его трудно прочесть. Но несмотря на это только блокчейн биткоина обработал почти миллиард транзакций. Когда дело доходит до эффективного расследования криптопреступлений, блокчейн-аналитика предоставляет правоохранительным органам преимуще-

---

[1] В 2023 году активность по отмыванию денег распространилась на большее количество депозитных адресов Сервисов, а также на новую тактику от Lazarus Group https://www.chainalysis.com/blog/2024-crypto-money-laundering/https://www.chainalysis.com/blog/2024-crypto-money-laundering/

ство, меняющее правила игры, поскольку она предлагает возможность анализировать обширные сетевые наборы данных, графические возможности для организации этих данных и контекстуализированное понимание незаконной криптоактивности.

Используя блокчейн-аналитику правоохранительные органы выявляют преступные организации, изучают активность в сети, такую как перемещение украденной или отмытой криптовалюты. Алгоритмы, поддерживающие эту технологию, собирают обширные сетевые наборы данных и предлагают возможности построения графиков, которые помогают правоохранительным органам визуально отслеживать движение средств с течением времени и связывать крипто-транзакции с объектами реального мира. Также блокчейн-аналитика помогает правоохранительным органам сопоставлять криптовалютные транзакции и представлять их в легко усваиваемом формате. Блокчейн-аналитика помогает правоохранительным органам продвигать расследования, задерживать преступников, представлять дела для судебного преследования и подготавливать пути для изъятия и возврата криптофондов жертвам, когда это возможно.

И хотя блокчейн-аналитика полезна для борьбы с преступностью, она также может помочь правоохранительным органам проявлять инициативу в предотвращении преступлений. Можно обнаружить незаконную деятельность на ранней стадии путем анализа моделей транзакций и взаимосвязей в цепочке, которые могут указывать на преступное поведение.

В 2020 году в России был принят закон «О цифровых финансовых активах» (ЦФА), которым был определён круг провайдеров ЦФА, но до сих пор в российском законодательстве не установлено, кто может выступать провайдером цифровых валют, в том числе криптовалют — есть лишь запрет для резидентов на использование цифровых валют в качестве средства платежа.

В России с начала 2021 года функционирует платформа «Прозрачный блокчейн», которая позволяет финансовой разведке анализировать крипто-транзакции. 1 июля 2022 года была запущена платформа центрального банка «Знай своего клиента», позволяющая анализировать финансовые транзакции банковских клиентов и относить их к одной из трех групп риска по возможной причастности к проведению сомнительных операций по принципу «светофора». Те, кто в результате анализа был отнесён к красному уровню риска, лишается возможности проводить платежи.[1]

В конечном счете, успешная борьба с криптопреступностью требует объединенных усилий государственных учреждений, правоохранительных органов и законодателей. Они играют важную роль в разработке, внедрении и обеспечении соблюдения криптополитики и нормативных актов, связан-

---

[1] Росфинмониторинг и банки научились отслеживать связи между банковскими операциями и криптовалютой https://3dnews.ru/1103836/servis-znay-svoego-kriptoklienta-pozvolit-viyavlyat-svyazi-megdu-tranzaktsiyami-v-kriptovalyute-i-s-obichnimi-dengami

ных с криптовалютами и технологией блокчейн. Этот единый подход является ключом к созданию безопасной, но инновационной среды, которая идет в ногу с быстрым развитием цифровых активов и технологии блокчейн.

Центральное место в арсенале правоохранительных органов по борьбе с криптопреступлениями занимает обмен блокчейн-разведкой между ведомствами. Такое межведомственное сотрудничество в сочетании со стратегическими государственно-частными партнерствами укрепляет нормативную базу и усиливает мониторинг соблюдения требований, тем самым играя важную роль в сдерживании и предупреждении преступности.

Подобно тому, как традиционные финансовые расследования являются рутинной обязанностью правоохранительных органов, расследования в области криптовалют должны стать такими же. Используя блокчейн-аналитику, правительственные учреждения могут активно отслеживать криптовалютные транзакции. Этот упреждающий мониторинг может помочь в предотвращении преступлений и обеспечить готовность агентств реагировать на значительные события в финансовой экосистеме — такие как введение санкций против крупных компаний или крах блокчейна, — которые могут повлиять на финансовую стабильность или создать системные риски.

Принятие этого упреждающего подхода, подкрепленного надежным надзором со стороны регулирующих органов, имеет решающее значение для поддержания целостности и безопасности криптоэкосистемы. Это подчеркивает важность регулирования и правоприменения в защите от угроз, создаваемых преступлениями с использованием криптовалют.

Блокчейн-аналитика играет решающую роль в борьбе с этими преступлениями. С усилением регулирования криптовалют правительствами и продолжающимся ростом внедрения цифровых валют необходимость борьбы с преступной деятельностью, основанной на криптовалюте, будет только усиливаться.

Литература

1. Аналитик блокчейна - кто это такой? [Электронный документ] https://coinkyt.com/article/analitik-blokchejna-kto-eto-takoj Дата ознакомления: 15.05.2024.

2. Тенденции криптопреступности 2024 года: незаконная активность снижается по мере сокращения мошенничества и кражи средств, но рынки программ-вымогателей и даркнета демонстрируют рост. [Электронный документ] https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ Дата ознакомления: 15.05.2024.

3. Криптовалютный скам, называемый «забоем свиней», проник в Apple App Store b Google Play Store. [Электронный документ] https://xakep.ru/2023/02/03/pig-butchering-in-app-stores/ Дата ознакомления: 15.05.2024.

4. В 2023 году активность по отмыванию денег распротранилась на большее количество депозитных адресов Сервисов, а также на новую тактику от Lazarus Group. [Электронный документ] https://www.chainalysis.com/blog/2024-crypto-money-laundering/https://www.chainalysis.com/blog/2024-crypto-money-laundering/ Дата ознакомления: 15.05.2024.

5. Росфинмониторинг и банки научились отслеживать связи между банковскими операциями и криптовалютой. [Электронный документ] https://3dnews.ru/1103836/servis-znay-svoego-kriptoklienta-pozvolit-viyavlyat-svyazi-megdu-tranzaktsiyami-v-kriptovalyute-i-s-obichnimi-dengami Дата ознакомления: 15.05.2024.

Назаров Артур Карапетович,
кандидат физико-математических наук
старший преподаватель
Краснодарского университета МВД России

НЕКОТОРЫЕ СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ОТ КИБЕРУГРОЗ

Современные киберугрозы постоянно усложняются. Поэтому задачи по киберзащите требуют постоянного совершенствования используемых методов и средств защиты. Так, например, на сегодняшний день очень актуальны средства поиска не детектируемых угроз в инфраструктуре организаций, противодействие атакам в режиме реального времени и максимально быстрое реагирование в случае инцидента. Среди таких современных средств защиты от киберугроз важно выделить XDR (от англ. Extended Detection and Response, «расширенные обнаружение и реагирование») — класс систем информационной безопасности, предназначенных для автоматического проактивного выявления угроз на разных уровнях инфраструктуры, реагирования на них и противодействия сложным атакам[1]. Например, такие системы могут содержат в себе так называемые песочницы – системы для выявления вредоносных программ, при использовании которой подозрительный объект запускается в виртуальной машине с полнофункциональной операционной системой, а для обнаружения зловредности объекта применяется анализ его поведения. Если объект выполняет вредоносные действия, песочница признает его вредоносной программой. Виртуальные машины песочницы изолированы от реальной инфраструктуры компании[2]. С помощью песочниц могут быть проверены не только файлы различных типов данных, которые могут содержать в себе активное содержимое (например, программы, установочные файлы и т.д.), но и ссылки (песочница переходит по url-адресу и выявляет загрузки, события JavaScript, исполнение Adobe Flash и др.).

XDR системы могут выполнять следующие действия:

- анализ сетевого трафика (анализ трафика, обнаружение аномалий, выявление скрытых каналов и т.д.);
- защита конечных станций и реагирование (сбор событий с хостов, сбор криминалистических данных, выявление атак в реальном времени и т.д.);
- детонация вредоносного программного обеспечения (поведенческий анализ, ретроспективный анализ);

[1] См. https://encyclopedia.kaspersky.ru/glossary/xdr-extended-detection-and-response/
[2] См. https://www.kaspersky.ru/enterprise-security/wiki-section/products/sandbox

- использование основанной на реальных наблюдениях базы знаний Mitre, содержащую описание тактик, приемов и методов, используемых киберпреступниками[1];
- использование известных методов определения поведения и стратегий, которые злоумышленник использует в кибератаке – TTPs[2];
- проактивный поиск не детектируемых угроз (анализ телеметрии, создание и тестирование гипотез и т.д.);
- реагирование на инциденты.

В силу постоянно растущего количества фишинговых и целевых атак возрастает также роль программ и других комплексов, обеспечивающих облачную защиту электронной почты. Такие системы позволяют выполнять следующие функции:

- атрибуция кибератаки – совокупность технических методов и организационных мероприятий, направленных на установление злоумышленника или преступной группировки, стоящей за кибератакой или вредоносной кампанией[3]. Для этого автоматически сопоставляются результаты детонации с облаком данных для проведения атрибуции атаки;
- ретроспективный анализ и обнаружение угроз – анализируется текст, ссылки, вложения, скачиваются объекты по имеющимся в письме ссылкам, затем они проверяются с целью обнаружения скрытых угроз;
- детонация нагрузок с помощью песочниц – максимально полное выполнение вредоносного кода в изолированный среде, затем формирование подробного аналитического отчета об угрозе и используемых техниках.

При использовании песочниц важно учитывать, что современные вредоносные программы анализируют свое окружение прежде, чем сами активизируют свои вредоносные функции. К примеру, они могут проверять название компьютера, имена пользователей, домены, сетевое окружение, объем оперативной памяти, установленные языки и т.д. Так, если какой-нибудь из таких параметров окажется подозрительным, например, объем оперативной памяти окажется менее 2 ГБ или среди установленных языков не будет русского языка и т.п., то вредоносная программа не выявит себя. Поэтому особенно необходимо, чтобы песочницы позволяли настраивать ключевые свойства виртуальных машин так, чтобы они выглядели максимально похожими на реальное окружение машин пользователей.

Среди популярных объектов атаки можно также отметить наличие сайта организации в сети интернет, который может оказаться каналом для доступа извне во внутреннюю инфраструктуру организации. Для защиты подобных систем необходимо проводить не только оценку уязвимостей, тести-

---

[1] См. https://encyclopedia.kaspersky.ru/glossary/mitre-attack/

[2] См. https://www.securitylab.ru/glossary/ttps/

[3] См. https://encyclopedia.kaspersky.ru/glossary/cyber-attribution/

рование на проникновение и другие традиционные методы обеспечение безопасности, но и использовать автоматизированные системы для анализа скрытых угроз внешнего периметра, проверки признаков подготовки хакерской атаки, выявления следов компрометации. Такого рода системы как правило позволяют выявлять не только критические уязвимости системы, сетевые уязвимости, но возможные утечки учетных данных, VPN-сервисы, некорректно настроенные базы данных и системы, забытые сетевые инфраструктуры, некорректные сертификаты, DNS-серверы и прочее.

Литература

1. Винокуров С. А. Основы кибербезопасности: учебник / С. А. Винокуров [и ДР]. – Воронеж. Воронежский институт МВД России, 2022. — 503 с.

2. Назаров А.К. Искусственный интеллект как фактор развития киберпространства // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму, г. Краснодар, май 2023. С. 58-59.

3. https://www.kaspersky.ru.

4. https://www.securitylab.ru.

Некрасов Денис Евгеньевич,
кандидат юридических наук, доцент,
профессор кафедры уголовного права и криминологии
Рязанского филиала Московского университета
МВД России имени В.Я. Кикотя

ПРЕДУПРЕЖДЕНИЕ ФОРМИРОВАНИЯ ЭКСТРЕМИСТСКИХ ВЗГЛЯДОВ ЛИЧНОСТИ

Развитие общественных отношений в условиях современных мировых процессов с неизбежностью ведет к усложнению восприятия и использования терминологического аппарата, призванного обозначать разнообразные, давно появившиеся или новые, явления. Так, широкую распространенность в использовании при оценке деяний и явлений разного рода в настоящее время получил термин «экстремизм». На разных уровнях общественного сознания он понимается как форма мышления, способ действия и даже образ жизни. Объединять такое многообразие его понимания и использования должно, прежде всего, то, что экстремизм в своих сущностных основах явление исключительно негативное и социально-опасное. Не смотря на то, что толковые словари разъясняют смысловое значение термина только как приверженность к крайним взглядам и мерам[1] без указания на отрицательное свойство, ему ни в коем случае нельзя придавать положительную оценку, тем более, переосмысливать историю применения.

В свою очередь, в законодательстве, направленном на борьбу с экстремизмом не дается его емкого и конкретного определения. В Федеральном законе «О противодействии экстремистской деятельности» оно закреплено путем перечисления ряда уголовно и административно наказуемых деяний, отнесенных к категории экстремистских[2]. В самом общем виде общеправовое определение экстремизма можно сформулировать как деятельность по планированию, организации, подготовке и совершению правонарушений, в крайних формах посягающих непосредственно на национальную и государственную безопасность, в том числе по мотивам политической, идеологической, религиозно-этнической и иной социальной ненависти либо вражды.

На государственном уровне борьба с экстремизмом и его проявлениями, оказывающими, прежде всего, дестабилизирующее влияние на общественно-политическую обстановку, ставится в качестве одной из приоритетных задач[3]. В этом плане, безусловно, важна предупредительная деятельность, особенно

---

[1] См.: Лопатин В.В., Лопатина Л.Е. Русский толковый словарь. М.: Русский язык, 1998. С.810.

[2] См.: Федеральный закон РФ от 25 июля 2002 года «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 2002. №30. Ст. 3031.

[3] См.: Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

ранняя профилактика, направленная на нейтрализацию формирования детерминант, побуждающих экстремистские проявления и способствующих им. Среди этих факторов большие опасения вызывает экстремистская идеология, распространение которой недопустимо. В Стратегии противодействия экстремизму в Российской Федерации до 2025 года указанная идеология охарактеризована как совокупность взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов[1]. В основе этих взглядов и идей лежит мотивация ненависти и вражды, как крайние формы неприятия объекта неустроенности их носителей. При этом, как считают специалисты, любое преступление, которое заключается, в частности, в передаче или (и) пропаганде идей, взглядов, направленных на возбуждение ненависти или вражды, а равно призывающих к ним, можно считать формой проявления, так называемого, идеологического экстремизма[2].

Среди особо опасных элементов подобной идеологии следует выделить экстремистские убеждения, то есть совокупность прочно сложившихся мнений, взглядов и точек зрения экстремистского характера. Соответственно лица, придерживающиеся этих убеждений, в целом являются потенциальными носителями угрозы общественной безопасности, особенно те, у которых укоренившиеся убеждения трансформировались в прочную систему установок – в экстремистский фанатизм. Такие личности, как правило, общеизвестны в лице лидеров и особо активных участников экстремистских формирований.

У любой личности, обладающей убеждениями имеется определенная линия (направленность) поведения, устойчивость и постоянство которой во многом зависит от степени укоренения этих убеждений в сознании. С другой стороны, формирующиеся у личности экстремистские убеждения могут сказаться на поведении далеко не сразу. Может пройти немалое количество времени, пока накапливающаяся «асоциальная энергия», в виде совокупности устоявшихся взглядов, мнений и т.д., выльется в конкретное деяние. Во многом это будет зависеть от разных субъективных факторов, и особенно от сложившегося конечного мотива, побуждающего к определенным действиям. В любом случае, степень готовности личности к экстремистскому акту будет тем выше, чем более устоялись соответствующие убеждения и окрепла уверенность человека в их состоятельности и необходимости придерживаться, следовать и даже отстаивать их противоправными мерами (что в конечном итоге и образует экстремизм). При этом свои внутренние убеждения данные лица демонстрируют, не только совершая преступления, но и посредством

---

[1] Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. 2020. №22. Ст. 3475.

[2] См.: Кочои С.М. Уголовно-правовое противодействие идеологическому экстремизму // Журнал российского права. 2021. Т. 25. № 11. С.124.

элементов, входящих в особую разновидность криминогенной субкультуры (татуировок, жестов, песен, лозунгов и т.д.), распространение которой, направлено на приобщение других лиц к данным взглядам.

В виду этого следует осознавать, насколько важно противодействовать формированию у личности экстремистских убеждений, по своей сущности являющихся продуктом крайне искаженной психологии и мировоззрения в области восприятия и соблюдения норм человеческого общежития. Отметим, что соответствующие убеждения, как и общая направленность личности, определяются потребностями и интересами, которые также складываются в ходе формирования личности[1]. Антиобщественные потребности и интересы уже сами по себе могут привести к выбору формы поведения, запрещенной законом и противоречащей нормам морали. В свою очередь, имеющиеся криминогенные убеждения могут выступить в роли катализатора и фиксатора подобного выбора.

К сожалению, многие факторы, существующие в современной действительности, способны породить или способствовать формированию деформированных потребностей и интересов. Для современного общества, несмотря на предпринимаемые меры, характерны не всегда положительные изменения в характере мышления и образе жизни. Правоохранительная практика, по-прежнему, констатирует снижение уровня правосознания, наличие правового нигилизма. Некоторые существовавшие положительные традиции, идеи и взгляды утрачиваются. Имеется достаточно широкий спектр неблагоприятных факторов, влияющих на становление личности, в том числе и нравственное, происходящее в течение всей его жизни. Одна из самых распространенных проблем большого количества членов современного общества – проблема психологического дискомфорта в социально-бытовой среде.

Не удивительно, что у некоторых индивидуумов, особенно у представителей подрастающего поколения, наблюдается либо недостаточное получение и закрепление необходимых социальных стереотипов, либо их искаженное восприятие. Между тем подобные пробелы у личности могут заполняться антиобщественными установками, убеждениями, в том числе и экстремистскими. Ситуация осложняется тем, что многие экстремистские акции направлены на призыв неограниченного круга лиц к осуществлению соответствующих действий, то есть носят пропагандистских характер. Отзываются на подобные призывы, как правило, именно формирующаяся личности несовершеннолетнего и молодежного возраста. При этом, если самим фактам публичных призывов, с учетом использования для их осуществления, как правило, информационно-коммуникационной среды, противодействовать достаточно сложно, то деятельность по недопущению «заражению» преподносимыми социально-опасными убеждениями системно выстроить возможно и необходимо.

---

[1] См.: Кудрявцев В.Н. Причины правонарушений. М.: Наука, 1976. С.96-115.

Поэтому одним из существенных шагов на пути системной профилактики рассматриваемого явления должно быть воспитание толерантности в обществе, нетерпимости к проявлениям экстремизма и т.д. Важное значение имеют также воспитательно-образовательные мероприятия и программы[1]. При этом указанное можно отнести к мероприятиям общесоциального уровня предупреждения экстремизма, поскольку перед этим процессом, помимо отмеченной, стоят и другие, в том числе более масштабные цели развития общества.

Однако, учитывая вышеизложенное, а также показатели преступности экстремистского характера, полагаем, что в настоящее время необходимо акцентировать внимание на осуществлении ряда мероприятий специально-криминологического уровня предупреждения формирования и распространения экстремистских убеждений и идеологии.

При разработке и применении данных мер необходимо исходить из того, что с одной стороны, экстремистские взгляды обеспечиваются соответствующей информацией и в этом же виде передаются, с другой стороны есть адресаты получения этой информации в виде конкретных лиц, которым она становится интересна. При этом наибольшую обеспокоенность должны вызывать случаи принятия, согласия личности с ней. Соответственно именно на носителей, потребителей и непосредственно экстремистскую информацию и необходимо направлять соответствующее предупредительное воздействие.

В свете отмеченного деятельность по предупреждению формирования и распространения экстремистских убеждений условно можно разделить на следующие группы: деятельность по нейтрализации имеющихся экстремистских потребностей, интересов и убеждений (у их носителей); деятельность по недопущению распространения указанных убеждений (направленные на недопущение распространения и восприятия экстремистских материалов, в т.ч. в ИТС «Интернет»; выявление и воздействие на лиц, поддерживающих и выражающих крайние взгляды; выявление лиц, осуществляющих призывы к осуществлению экстремистской деятельности; обеспечение соблюдения законодательства о публичных мероприятиях).

Сегодня следует констатировать наличие особых составляющих общественной опасности экстремизма в сети Интернет, где он имеет организованный и публичный характер, формирует в обществе устойчивые экстремистские движения, сопровождаемые попытками их легализации, в т.ч. на международном уровне. Все чаще контент сети «Интернет» становится руководством к действию. Указанное определяет особые признаки в современной «цене» экстремизма, что влияет и на выбор механизмов противодействия – преимущественно, уголовно-правовых.

---

[1] См.: Родина М.Е. Основные направления противодействия экстремизму // Российский следователь. 2016. N 15. С. 41 - 44.

Информационно-коммуникационные технологии облегчили поиск «единомышленников», при этом важным является понимание возможности оставаться анонимным, не быть идентифицированным по социально-демографическим признакам, подлежащим государственному учету. Это, в свою очередь, является существенным условием для правонарушающей деятельности.

Как видим, немаловажную роль в механизме противодействия экстремизму следует отводить исследованию психологических аспектов процесса распространения экстремистских убеждений, как правило, осуществляемого участниками экстремистских группировок в целях пополнения своих рядов новыми членами. Люди, впервые приобщенные к крайне асоциальным взглядам и установкам становятся своеобразными жертвами экстремизма «первой волны», поскольку причиняется ущерб их здоровому мировоззрению. В последующем подобные индивидуумы осуществляют, либо в любое время готовы совершить административно или уголовно наказуемый экстремистский акт, причиняя тем самым прямой ущерб охраняемым соответствующим законодательством общественным отношениям, порождая потерпевших «второй волны». Полагаем, что данные положения следует учитывать при исследовании виктимологического аспекта противодействия экстремизму, а так же механизма предупреждения формирования экстремистских установок и убеждений.

Петров Семен Александрович,
кандидат технических наук,
доцент Краснодарского университета МВД России

Аула Александра Денисовна,
курсант
Краснодарского университета МВД России

АНАЛИТИКА ПЕРСПЕКТИВ РАЗВИТИЯ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

В современном цифровом мире киберпреступность стала серьезной угрозой для государства, организаций и частных лиц. Информационные атаки стали более утонченными и сложными. В условиях быстрого развития цифровых технологий, интернета и информационных систем киберпреступность становится более сложной и разнообразной, поэтому важно иметь механизмы для выявления таких атак, для этого необходимо разбираться в кибератаках, знать их аналитику и предугадывать прогноз на ближайшие годы. В данной статье представлены аналитические данные киберпреступности в современном мире.

Для понимания важности защиты информационных, компьютерных систем необходимо знать статистику совершенных киберпреступлений в разных сферах. Для возможности прогнозирования атак на сферы деятельности необходимо провести анализ угроз на малый бизнес, государственный сектор и сферу IT-преступлений.

В сфере малого бизнеса важно отметить, что число атак на *Российские* информационные системы в 2023 году выросло на 65%, в то время как за первый квартал этого же года уже было выявлено 53% от общего числа атак за весь год. Ситуация в 2022 году была лучше, чем в 2021 году. В 2022 году 22% от общего числа преступлений за год, в то время как в 2021 году представлена почти половина преступлений направлена на информационную сферу, что составляет 47%. А связано это с тем, что в 2020 году начался процесс входа в виртуальный мир. Одна из основных причин – Карантин, он заставил большую часть работы в офисах перенести на уделенный вид работы, что позволило злоумышленникам расширить сферу своего влияния на компьютерные системы, так как сотрудники офисов еще не были знакомы с новым видом преступлений и часто переходили на ссылки от злоумышленников, чем позволяли вторым завладеть информацией.

Так за 2020 год было совершено 37% от всех преступлений за текущий год. В сравнении с 2018 годом, в котором было совершено только 30% таких преступлений, можно отметить значительный прирост. Поэтому необходимо ответственно подходить к использованию личной информации внесенной в свой компьютер.

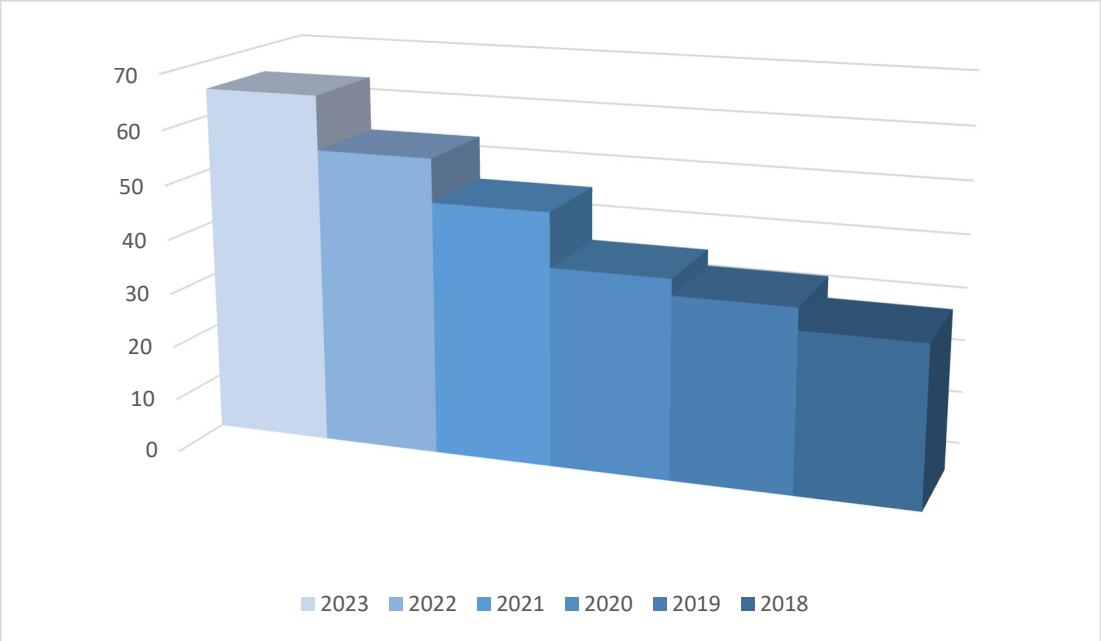


Рис. 1. Атаки на КИИ в бизнес секторе в %.

Отчет компании "РТК-Солар" выявил что, во втором квартале 2023 года было выявлено 325 тысяч инцидентов в области информационной безопасности. Это на 12% больше, чем в первом квартале и на 38% превышает показатель аналогичного периода прошлого года. Тенденция на увеличение числа инцидентов, сформировавшаяся еще в конце прошлого года, не только сохранилась, но и усилилась: с 3% в первом квартале до нынешних 12%. Количество подтвержденных угроз из всего объема выявленных событий составило 8850 случаев. Прирост составил 24% по сравнению с первым кварталом 2023 года.

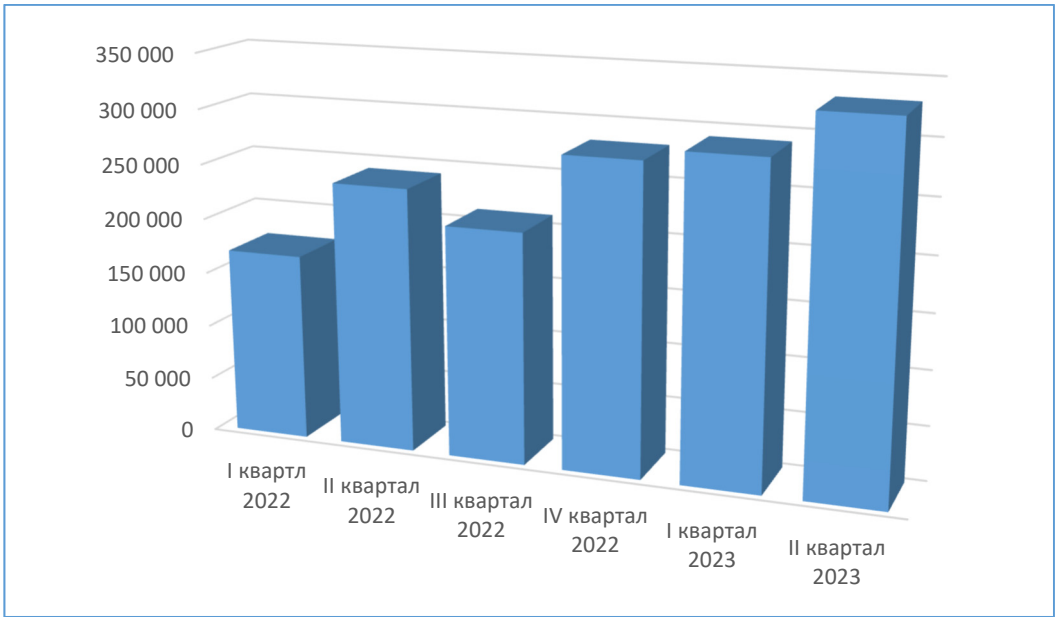


Рис. 2. Общий прирост инцидентов в области информационной безопасности

Аналитики утверждают, что помимо прирост атак злоумышленников в количественном отношении происходит изменение вектора направленности. Как показывают отчеты компаний, применение вредоносного ПО - наиболее частый инструмент (53% всех инцидентов) в руках хакеров, который приводит к наступлению критических инцидентов. Из них 36% были связаны с применением шифровальщиков, что на 26% превышает аналогичный показатель первого квартала 2022 года.

На первое место среди средств защиты выходят устройства IoT, межсетевые экраны и искусственный интеллект. Опасность состоит в том, что через устройства IoT можно совершить несанкционированный взлом в программное обеспечение компании.

Подобных инцидентов на *Российском* рынке в 2023 году было рекордное количество – 5532. Это в 2,4 раза больше, по сравнению с данными 2022 года.

В 2023 году хакерские атаки с помощью IoT-устройств коснулись малого бизнеса. Порядка 60% предпринимателей полагаются на антивирусные программы, не нанимая персонал, специализированный на кибербезопасности, в целях уменьшения расходов, но за этим стоят неимоверные потери как в денежной базе, так и в клиентской. Как итог, в 71% случаев они становятся жертвами нецелевых атак.

Доля атак, мотивом которых была финансовая выгода, выросла — с 37% в 2020 году до 47% в 2021, в настоящее время показатели только возрастают. Этому поспособствовало обилие злоумышленники распространяют шифровальщики, что расширяет количество совершенных атак.

Государственный сектор занимает 15% от всех реализованных успешных атак на различные отрасли за первые три квартала 2023 г. Данный показатель на 3% меньше, чем в 2022 г.

ВПО (Вредоносное программное обеспечение) использовалось в каждой второй атаке, что демонстрирует небольшое повышение по сравнению с 2022 г. Стоит отметить, что, помимо шифровальщиков (вирус, который шифрует файлы на компьютере и лишает владельца доступа к ним) и ВПО для удаленного управления, в 2023 г. популярностью у злоумышленников пользовалось шпионское ПО (программа, которая следит за онлайн-активностью в тайне от лица), что в целом соответствует общим трендам 2023 г. Распространение ВПО в государственных организациях осуществлялось в основном через электронную почту и при компрометации компьютеров, серверов и сетевого оборудования.

Социальная инженерия как метод атаки в 2023 году отмечалась в 42% успешных атак на государственные организации, что сопоставимо с ситуацией в 2022 г. Эксплуатация уязвимостей на внешнем сетевом периметре компаний составила 24%.

Последствия атак на Гос. сектор могут сказаться на критически важных государственных услугах и вызвать утечку как персональных данных,

так и другой конфиденциальной государственной информации. Кроме того, количество инцидентов будет только расти.

За последние годы, согласно статистическим данным, мы видим, что стоимость утечки информации растет. С 2020 года рост составляет 15,3%. Также растет и количество крупных атак. В 2020 их насчитывалось 1120, а уже в 2023 – 1659. Конечно, увеличение количества утечек влияет и на размер убытков от них.

Количество атак выросло до 1661 по состоянию на конец ноября. По сравнению с 2022 годом это на 10% больше. 2023 год поразил количеством майских атак с утечкой данных, что прямо повлияло на резкую динамику, однако в целом количество атак растет плавно. Вероятнее к кону 2024 году количество атак будет увеличиваться, но все же плавно.

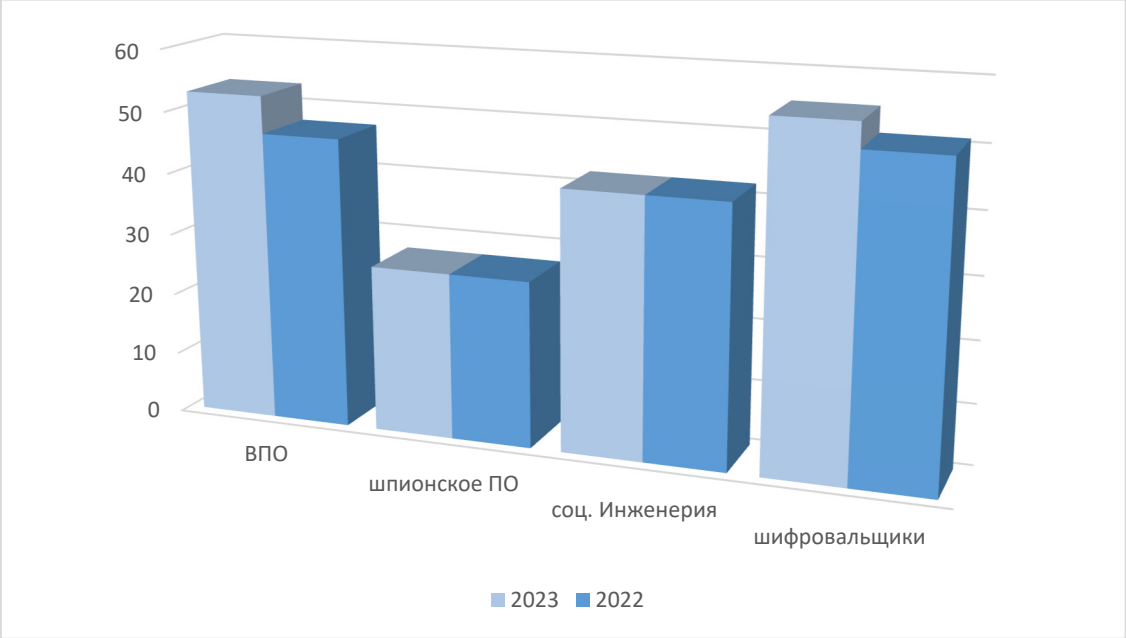


Рис. 3. Атаки на КИИ в Гос. секторе в %.

В ближайшем будущем Государственные организации России столкнутся с увеличением количества высококвалифицированных целевых атак. С помощью специальной военной операции создалась возможность для того, чтобы группировки хорошо подготовились к целевым атакам на государственный сектор и его важные ресурсы. Количество инцидентов будет только расти, а государственные организации в России столкнутся с увеличением количества высококвалифицированных целевых атак, так можно предположить, что в 2024 году процент атак будет составлять 20-25 % от общего числа атак. Согласно аналитике центра исследования киберугроз "РТК-Солар", в 2023 году общая доля сложных атак составила 20% от всех расследуемых инцидентов.

Аналитики утверждают, что в 2024 году нас ожидает увеличение количества кибератак в следствии консолидации киберггруппировок и глобальных соглашений между странами. Так же предполагается увеличение попыток проведения атак на цепочки поставок.

В области IT сферы в 2024 году мы продолжим наблюдать бурный рост и появление еще большего количества продуктов в кибербезопасности, которые имеют ИИ. В последние годы киберпреступники все чаще используют новые инструменты, включая искусственный интеллект и машинное обучение, для проведения многочисленных кибератак. Такая тактика киберпреступников усиливает необходимость в разработке инновационных решений, соответствующих масштабу и серьезности угроз. Этот процесс напоминает гонку вооружений, где, с одной стороны, находятся атакующие, а с другой – защитники, но все происходит в ИТ-инфраструктуре государственных и бизнес-систем.

Необходимость в продуктах кибербезопасности на основе ИИ существует, но при этом остается открытой проблема доверия к решениям на базе искусственного интеллекта. Несмотря на успех многих приложений машинного обучения, в реальных условиях они не всегда оправдывают ожидания. Большое количество проектов в области машинного обучения неудачно завершаются, и многие концептуальные разработки так и не доходят до производства. Проблема в том, что разработчики нейросетей и классификаторов уделяют больше внимания построению моделей, чем их реализации в продукте. Многие компании-разработчики нанимают специалистов Data Science, которые потом делают модели обнаружения на общедоступных наборах данных, по сути являющихся часто мусором. Специалисты по DS не являются экспертами в ИБ и не в состоянии понять качественные ли данные или нет.

В 2024 году основной проблемой разработки в кибербезопасном ИИ станет кадровый разрыв. Компаниям-разработчикам нужны междисциплинарные специалисты, эксперты по созданию моделей обнаружения атак, которые сами в состоянии атаку сделать и оценить качество набора данных.

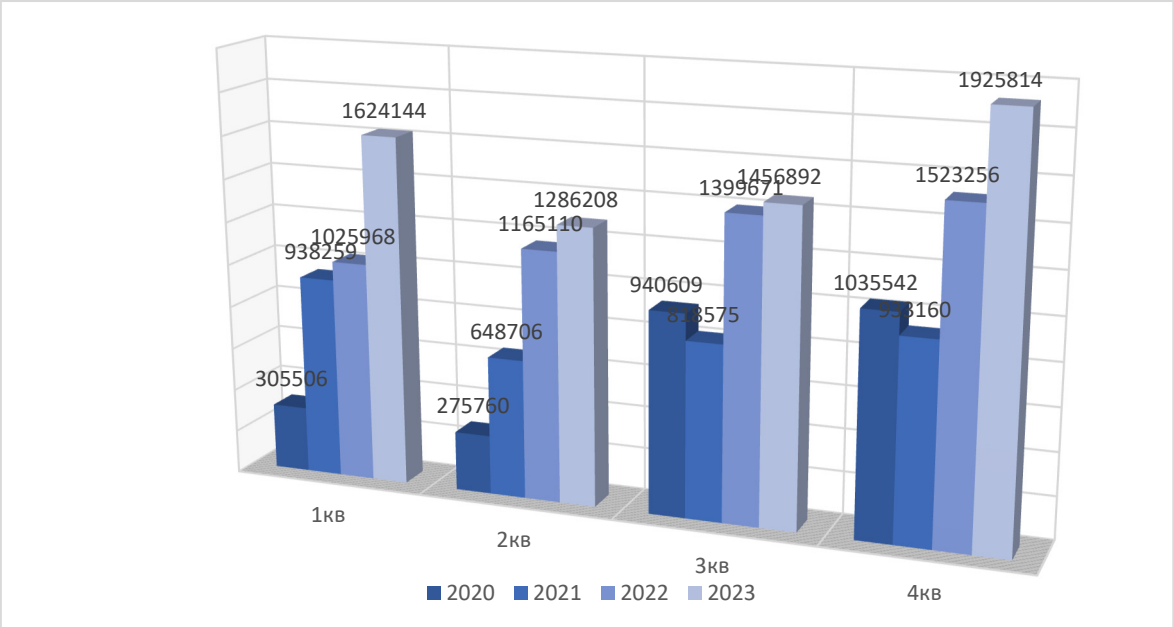


Рис. 4. Поквартальный объем мировых фишинговых атак за 2020-2023 гг.

В заключении стоит отметить, что количество атак в виртуальной сфера будет расти, а это на прямую связано с желанием злоумышленников завладеть данными, для чего они используют компьютерные технологии, которые с каждым днем усовершенствуются и набирают обороты развития. Так происходит становление новых видов преступлений в новой сфере влияния на общество. Следовательно, правоохранительным органам необходимо обеспечивать своевременный отклик на угрозы в сфере информационной безопасности, развивать и квалифицировать свою деятельность, не только в реальном мире, но и в виртуальном.

Литература

1. https://www.ortivus.com/mfn_news.
2. https://tass.ru/ekonomika.
3. https://www.tadviser.ru.
4. https://aerissecure.com

Победа Александр Сергеевич,
заместитель начальника кафедры
информационной безопасности
Краснодарского университета МВД России

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ С ПОМОЩЬЮ АВТОМАТИЗИРОВАНЫХ УТИЛИТ

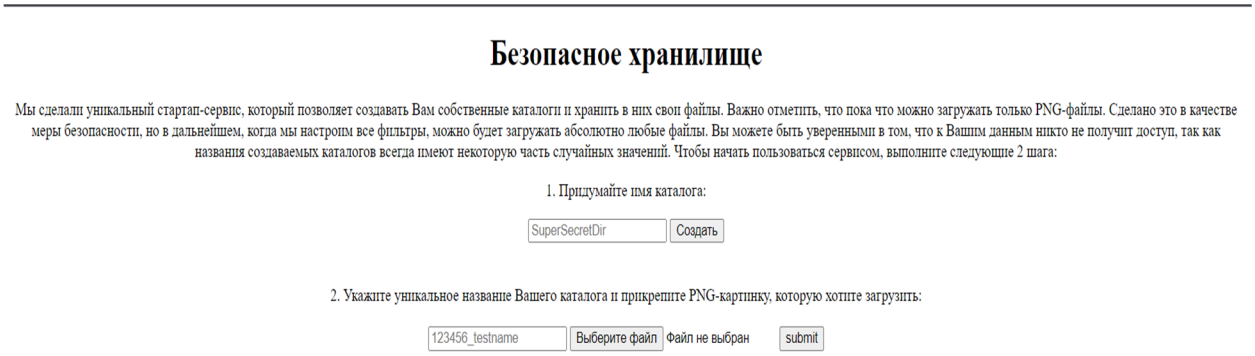
Безопасность веб-сервисов в сети Интернет всегда являлась актуальным вопросом, так как все коммерческие компании и государственные структуры используют в своей повседневной деятельности сетевые технологии.

Обработка персональных данных, внедрение платежных систем, базы данных и др., все это непосредственно интегрировано в современные веб-сервисы. Все крупные производственные предприятия прибегают к использованию сетевой инфраструктуры в своей деятельности для автоматизации процесса производства. Тем самым должен быть обеспечен высокий уровень безопасности организации как изнутри, так и снаружи.

Одним из важных элементов аудита безопасности информационной системы выступает pentest (penetrating testing «тестирование на проникновение»). Данная задача может быть реализована как силами специалистов внутри самой организации, так и независимой сторонней организацией с целью выявления различных точек входа в информационную сеть компании, с помощью которых можно нанести значительный ущерб путем завладения автоматизированными рабочими местами или серверами для деструктивного воздействия на систему или компрометации данных.

Существует большое количество инструментов, которые позволяют выявить потенциальные угрозы для эксплуатации информационной системы. Поэтому нужно перебирать все возможные сценарии для проведения атаки, для этого необходимо выявить всевозможные ключевые точки, начиная от информации, которая связана с доменными именами организаций, заканчивая критическими уязвимостями, вызванными сложной конфигурацией системы или ошибками, допущенными на этапе программной разработки или интеграции различных служб в единую систему. Ключевым аспектом, на который нужно ориентироваться, является список OWASP TOP 10, в котором представлены наиболее распространенные уязвимости за выбранные периоды (обновление списка осуществляется каждые 4 года).

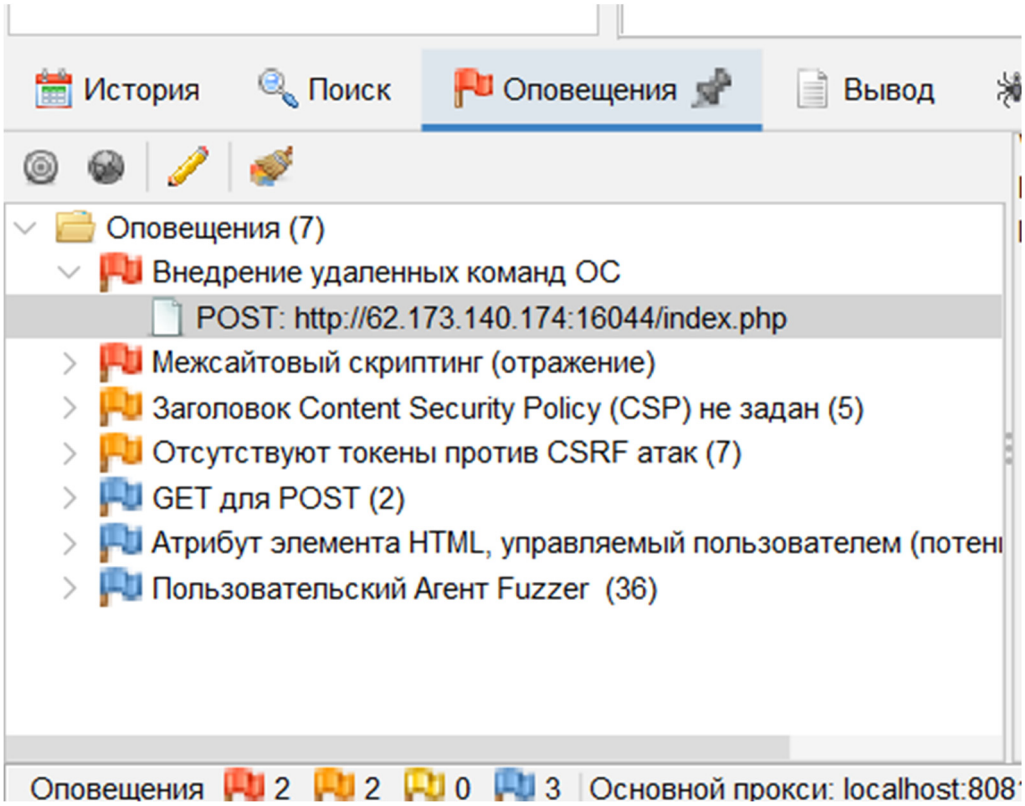
На примере нескольких инструментов рассмотрим примерный алгоритм тестирования веб-сервиса на открытой платформе codeby.games. Данный ресурс предназначен для улучшения своих навыков специалиста по защите информации. Задание представляет собой простой сервис для хранения файлов.



Для начала воспользуемся инструментом dirsearch для поиска скрытых директорий. Пример простой команды выглядит так **dirsearch -u (**ссылка на сайт).

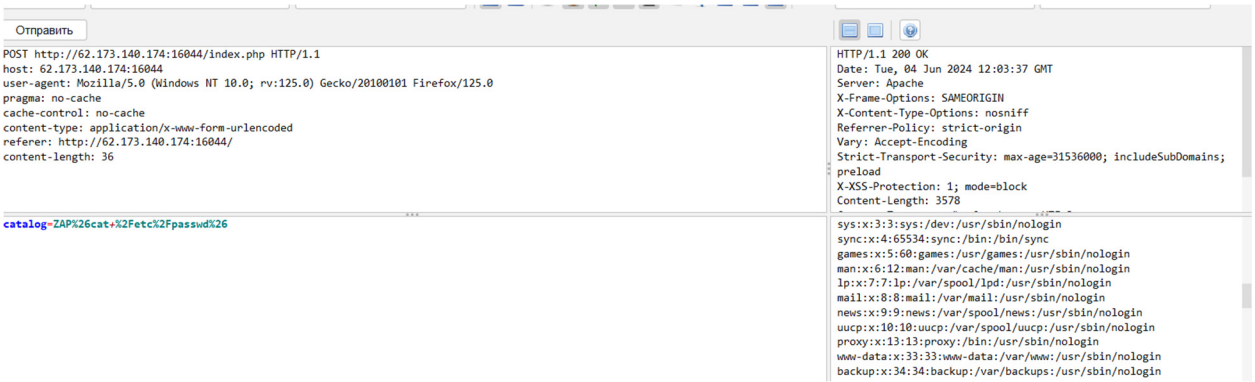
```
Target: http://62.173.140.174:16044/

[15:19:47] Starting:
[15:19:51] 403 -  266B  - /.ht_wsr.txt
[15:19:51] 403 -  266B  - /.htaccess.sample
[15:19:51] 403 -  266B  - /.htaccess.orig
[15:19:51] 403 -  266B  - /.htaccess.bak1
[15:19:51] 403 -  266B  - /.htaccess.save
[15:19:51] 403 -  266B  - /.htaccess_extra
[15:19:51] 403 -  266B  - /.htaccess_orig
[15:19:51] 403 -  266B  - /.htaccessOLD
[15:19:51] 403 -  266B  - /.htaccessBAK
[15:19:51] 403 -  266B  - /.htaccess_sc
[15:19:51] 403 -  266B  - /.htaccessOLD2
[15:19:51] 403 -  266B  - /.htm
[15:19:51] 403 -  266B  - /.html
[15:19:51] 403 -  266B  - /.htpasswd_test
[15:19:51] 403 -  266B  - /.htpasswds
[15:19:51] 403 -  266B  - /.httr-oauth
[15:19:52] 403 -  266B  - /.php
[15:20:04] 200 -    2KB - /index.php
[15:20:04] 200 -    2KB - /index.php/login/
[15:20:04] 301 -  314B  - /javascript  ->  http://62.173.140.174:16044/javascript/
[15:20:10] 403 -  266B  - /server-status
[15:20:10] 403 -  266B  - /server-status/
```

Результаты сканирования не показали ничего необычного, доступ к большинству файлов ограничен. Воспользуемся комплексным решением под названием Owasp ZAP для полного сканирования веб-сервиса.

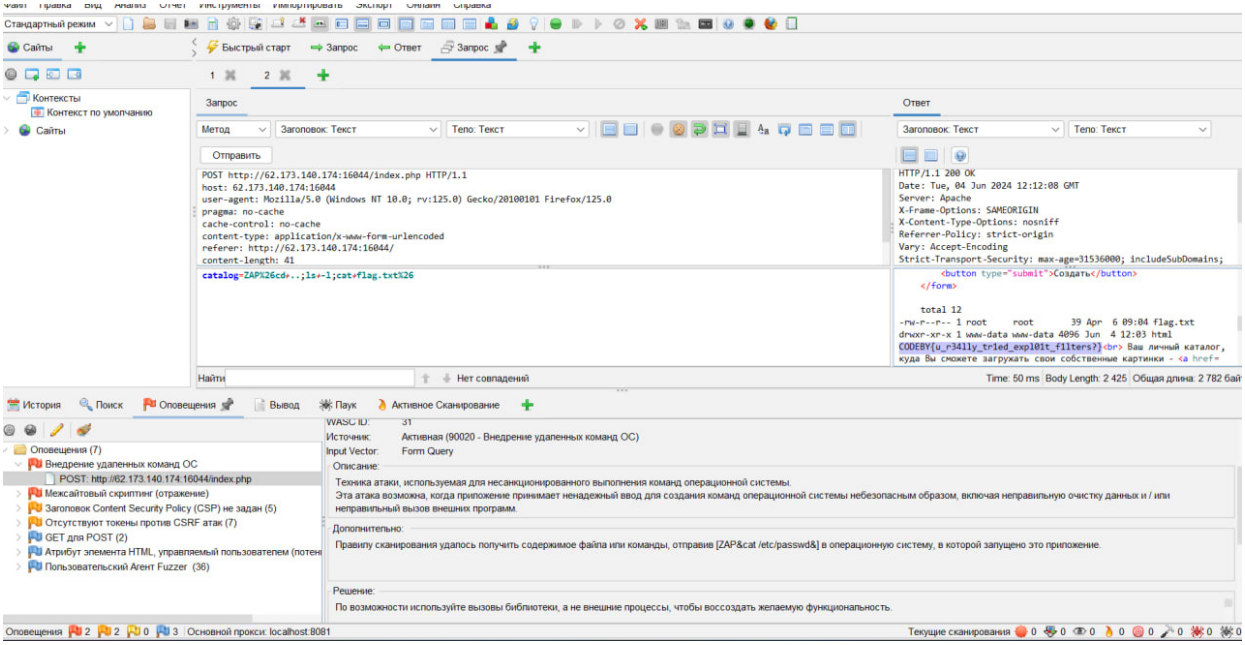


По результатам сканирования было выявлено две критические уязвимости: межсайтовый скриптинг, который позволит злоумышленнику внедрить в выдаваемую веб-системой страницу вредоносный код, и внедрение удаленных команд, с помощью которых можно манипулировать действиями на целевом сервере, на котором расположен сайт.

Просмотрев запрос, видим, что сканеру удалось заполучить содержание файла etc/passwd, что является недопустимым в рамках безопасности системы.



Обнаружив входную точку в POST запросе в параметре catalog и продолжив манипуляции, не составляет труда получить решение к этой задаче, которое находится в каталоге ниже в flag.txt.



В ходе реализации базовой задачи был разобран примерный алгоритм действий для тестирования веб-приложения, а также подтверждена вся серьёзность и важность данного процесса при обеспечении безопасности.

Литература

1. Codeby Games. Теория с практикой. Режим доступа: https://codeby.games/

2. Что такое пентест: описание, виды и где найти практику. Режим доступа: https://codeby.school/blog/informacionnaya-bezopasnost/ID-chto-takoe-pentest-i-zachem-on-nyzhen

3. Тестирование на проникновение. Эффективность vs популярность. Режим доступа: https://kontur.ru/articles/1673

Победа Александр Сергеевич,
заместитель начальника кафедры
информационной безопасности
Краснодарского университета МВД России

Роженцева Маргарита Алексеевна,
курсант Краснодарского университета МВД России

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ОРУДИЕ БОРЬБЫ ПРОТИВ ЭКСТРЕМИЗМА

Экстремизм является одной из самых сложных и актуальных проблем в настоящее время. Он представляет собой угрозу и опасность для безопасности государства, общества, разрушает социальный строй и вызывает большие человеческие и экономические потери. Поэтому с этим возникает необходимость в создании новых способов и методов для борьбы с экстремизмом. В данной статье, рассматривается способ использования искусственного интеллекта в борьбе с экстремизмом.

Для того, чтобы точно разобраться как используют искусственный интеллект против экстремизма необходимо разобрать понятие «экстремизм». Обращаясь к Федеральному закону от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» под экстремизмом понимается:

- насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации, за исключением делимитации, демаркации, редемаркации Государственной границы Российской Федерации с сопредельными государствами;
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;

Искусственный интеллект влился всецело в современное общество. На данный момент его используют в абсолютно разных сферах как главного помощника. В России каждый человек осознает и понимает весь потенциал искусственного интеллекта, поэтому предпринимают определенные меры для его регулирования. В 2019 году был принят Указ Президента Российской Федерации №490 «О развитии искусственного интеллекта в Российской Федерации», который определил основные понятия, цели и задачи государственной политики в этой области. В Указе указано официальное понятие:

«Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.» Таким образом искусственный интеллект захватывает большую часть технологий. В него входят алгоритмы, которые могут учиться на данных и делать прогнозы или принимать решения без явного программирования, что в целом упрощает его использование человеком. Поэтому важно отметить, что это умнейшая технология, которая может упростить жизнь во всех сферах жизнедеятельности общества. Однако следует использовать ее ответственно и нравственно. Так как если использовать данную систему в незаконных целях и со злым умыслом, то возможно совершение преступных деяний и потери контроля над искусственным интеллектом. Что повлечет за собой лишь разрушения и дестабилизации общества.

Если задумываться про то, как же использовать искусственный интеллект против экстремизма, то самое первое слово приходит на ум: «прогноз». То есть, использование методов прогнозирования. Прогнозирование является одним из важных элементов искусственного интеллекта. Оно способствует предотвращению экстремистских действий, предупреждает о возможных угрозах государству и общества. Помимо всего искусственный интеллект способен выявлять лица, которые наиболее уязвимы для экстремизма. Использование умной машины в борьбе с экстремизмом сосредоточено на создании точных прогнозов, которые помогают более эффективно направлять ресурсы на борьбу с возможными угрозами. Таким образом, искусственный интеллект с помощью использования метода прогнозирования, является средством улучшения распределения ресурсов для борьбы с экстремизмом.

В настоящее время очень часто можно встретить экстремистскую деятельность в социальных сетях. Специалисты информационной безопасности выяснили, что большинство групп в социальных сетях с экстремистской деятельностью отсутствуют в свободном доступе. Поэтому была создана группа под руководством H. Chen куда входят множество организаций, которые противостоят экстремизму на протяжении несколько лет и у них есть материалы разных форумов, блогов, статьей и так далее. Из всего этого собралась огромная база, которая содержит в себе 3 миллиона постов с 29 международных форумах на множествах языках мира. Естественно база каждый раз обновляется. Внедрение этой базы в искусственный интеллект позволяет вычислить основные лозунги и статьи, призывающие к экстремистской деятельности. Он способен вычислять активность в социальных сетях, форумах и других онлайн-платформах, выявляя подозрительные сообщении и профили.

Так же следует отметить то, что искусственный интеллект умеет распознавать содержание аудиозаписей и видеозаписей. Это очень важно, так как экстремисты используют абсолютно разный мультимедийный контент для продвижения своей идеологии и целей. Поэтому существует такая способность у искусственного интеллекта выявлять экстремистские высказывания, анализировать лицевые признаки и сопоставлять их с базами данных.

Примером использования искусственного интеллекта можно отметить проект «Counter Extremism Project». Это инициативная группа, которая совершает мониторинг и анализ экстремистского контента в интернете. CEP разрабатывает всевозможные алгоритмы, способные выявлять пропагандистские материалы и блокировать их распространение. На данный момент таких групп и систем создается множество. Таким образом, каждая группа берет свое направление и использует различные способы по выявлению и предотвращению экстремизма.

Искусственный интеллект представляет собой сильное орудие в борьбе с экстремизмом. Однако, его нужно правильно использовать и ставить определенные ограничения, чтобы не нарушались основные права и свободы человека и гражданина. Его возможности по мониторингу, анализу и прогнозированию делают незаменимым помощником для органов внутренних дел и других организаций, которые занимаются обеспечением безопасности общества и государства.

Литература

1. Статья из интернета, сайт securityLab дата публикации 30.05.2023 г. «Опасная тенденция: генеративный ИИ и его роль в создании контента, подстрекающего насилие и экстремизм» [Электронный ресурс] URL: https://www.securitylab.ru/news/538543.php
2. Статья «Искусственный интеллект и противодействие экстремизму» О. Б. Березина [Электронный ресурс] URL: https://sgugit.ru/upload/science-and-innovations/conference-ssga/international-scientific-methodical-conference-actual-problems-of-education/collections-of-materials-nmk-2023/part3/212-215.pdf
3. Федеральный закон от 25.07.2002 г. №114-ФЗ «О противодействии экстремистской деятельности» | КонсультантПлюс [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_37867/2daf50f586c69eac11512c1faa4309699b52ec9b/
4. Указ Президента Российской Федерации от 10.10.2019 г. №490 «О развитии искусственного интеллекта в Российской Федерации» (с изменениями и дополнениями) | ГАРАНТ [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_335184/
5. ГОСТ Р 51275-2006 Национальный стандарт «Защита информации», «Объект информатизации. Факторы, воздействующие на информацию» от 01.02.2008г. [Электронный ресурс] URL: https://docs.cntd.ru/document/1200057516
6. Федеральные закон «О полиции» от 07.02.2011 г. №3 статья 10 «Взаимодействие и сотрудничество» | КонсультантПлюс [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_110165/
7. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) | КонсультантПлюс [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/

Победа Александр Сергеевич,
заместитель начальника кафедры
информационной безопасности
Краснодарского университета МВД России

Савицкий Игорь Романович,
командир отделения Краснодарского университета МВД России

АНАЛИЗ МЕТОДОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ВОЗДЕЙСТВИЙ

В современном мире, где информация распространяется почти мгновенно и охватывает миллиарды людей, информационно-психологическое воздействие становиться мощным инструментом влияния на социальную и внутриполитическую деятельность государств. Информационные войны, манипуляции сознанием, целенаправленное распространение дезинформации и другие методы информационно-психологического воздействия активно используются для дестабилизации внутренней обстановки в странах мира. Эти воздействия могут иметь самые разнообразные формы и методы, начиная от пропаганды и заканчивая кибератаками, направленными на подрыв доверия к государству или государственным структурам.

Информационно-психологическое воздействие – это комплексное воздействие, включающее как информационные, так и психологические методы, с целью влияния на общественное мнение и поведение людей. В основном распространяется в социальных сетях и средствах массовой информации, но может выставляться и просто в сети интернет для создания помех получения достоверной информации.

Пропаганда представляет собой систематический комплекс сред распространения информации, идей и слухов с целью формирования общественного мнения и настроения в нем в интересах определенной группы или идеологии.

Одним из видов информационно-психологического воздействия является рекламное влияние, оно представляет совокупность различных видов манипуляции, таких как:

1) Эмоциональное воздействие, оно может выражаться в рекламном ролике акцентируемом на определенной эмоции страх, грусть, ненависть и тому подобное.

2) Психологическая манипуляция использует метод социального доказательства или авторитетную фигуру для создания видимости правдивости сказанных слов, хотя на самом деле они таковыми не являются.

3) Символическое воздействие или создание ассоциаций это метод предполагающий создания у людей через рекламные ролики образа такого мышления, что у граждан появляются образы хорошей жизни

Еще одним видом воздействия на сознание общественности является политическое воздействие, оно является очень действенным, так как исходит от самого государства и влияет напрямую на настроения общественности и при этом создает в нем же волнения. Методами такого воздействия могут послужить:

1) Манипуляция информацией, то есть выборочное представление фактов или ложной информации, которая влияет на формирование мнения о политике или событиях. Иными словами можно сказать, что это не только жесткая цензура предоставляемой гражданам информации, но и представление информации в выгодном для государства свете.

2) Манипуляция эмоциями использует страх, гнев или надежду для поддержки политических идей государства или его лидера.

3) Психологическое влияние через обещания предполагает воздвижения надежд на будущее у гражданского населения, о решении насущных проблем или улучшение качества жизни. К сожалению эти обещания хоть и выглядят маняще, но это всего лишь ловушка, которая захлопнется после принятия того или иного решения за которое было дано это обещание, ведь оно вряд ли будет исполнено в полной мере как было сказано, а лишь частично удовлетворив желания лишь некоторых, для предотвращения возмущения больших групп людей.

Воздействие средств массовой информации подразумевает под собой использование популярных личностей для пропаганды или настройки под свой лад массы людей, методами может являться:

1) Формирование общественного мнения, а именно чрезмерное освещение определенных событий для формирования определенного мнения или реакции общества на эти события.

2) Использование поведенческих паттернов представляет собой создание программируемых реакций с помощью виртуализированных форматов программ и новостных сюжетов, создание видео роликов с реакцией на то или иное событие для перенастройки сознания населения атакуемого государства.

3) Эксплуатация внушаемости, этот метод использует психологические способы воздействия, для формирования определенных настроений в обществе.

Социальное воздействие оказывает свое влияние на определенную группу людей, так как она влияет более точечно нежели другие информационно-психологические воздействия направленные на дестабилизацию, методами могут послужить:

1) Использование групповой динамики – это представление сообщений или действий подходящих под ожидания общественности, то есть влияние на восприятие той или иной информации.

2) Воссоздание групповой идентичности иначе говоря подчеркивание сходства и принадлежности к определенной социальной группе для усиления воздействия на мировосприятие этой группой.

3) Использование авторитетов, то есть внушение заведомо ложной информации или продвижение незаконных действий путем оглашение такой информации авторитетной личностью.

Таким образом, информационно-психологическое воздействие затрагивает широкий спектр методов, направленных на изменение сознание, поведения и убеждения людей через различные каналы и стратегии. Эти методы могут быть применены как отдельно, так и в комплексе, для достижения максимального эффекта и контроля над общественным мнением и поведением.

Литература

1. Чугунов А.В. Цифровая пропаганда и общественные настроения. Издательство «Проспект», 2018 г. -896 с.

2. Махов С.Ю., Еремин Р.В. Информационно-психологическая безопасность личность // Орловский юридический институт МВД России 2020 г. -184 с.

3. Баришполец В.А. Информационно-психологическая безопасность основные положения // Вычислительный центр им. А.А. Дородницына РАН. Москва, Российская Федерация 2012 г. -104 с.

Руднев Артем Игоревич,
преподаватель
Краснодарского университета МВД России

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ НА ОБЪЕКТАХ ТРАНСПОРТА

На сегодняшний день, международные террористические и экстремистские организации, радикально настроенные группировки, интенсивно используют имеющиеся телекоммуникационные технологии, для оказания информационного и психологического воздействия на граждан Российской Федерации, особенно молодое поколение (школьников, студентов и др.). Данная категория граждан России, легко подвержена вышеуказанному виду воздействия, т.к. у каждого имеется устройство с выходом в сеть «интернет», будь то (телефон, планшет, ноутбук, ПК и т.д.), в котором установлены различные мессенджеры, приложения и социальные сети, а также имеется различная информация личного характера. Это персональные данные, фотографии, данные родственников, друзей, знакомых и другая различная информация, которая при использовании определенных программ может попасть в руки данных организаций и группировок и в дальнейшем быть использована в своих целях. В связи с этим, государство уделяет особое внимание «молодежному экстремизму».

В целях предотвращения, фактов вовлечения молодых граждан России в террористическую и экстремистскую деятельность и совершения ими каких-либо других противоправных действий (деяний), проводится постоянный мониторинг сети «интернет». Сотрудниками ОВД и Росгвардии, организовываются выборочные проверки учащихся в образовательных учреждениях (школах, лицеях, колледжах профессионального обучения, институтах, академиях, университетах и т.д.) и самих учреждений, в целях проверки готовности к чрезвычайным ситуациям, ведется профилактическая работа с несовершеннолетними сотрудниками ПДН, как территориальных органов, так и транспортной полиции, благодаря чему в большинстве случаев удается пресечь правонарушения вышеуказанной категории граждан.

В настоящий момент, самой приоритетной задачей, органов государственной власти и правоохранительных органов, является противодействие экстремизму и терроризму, связанное с выявлением и пресечением причин, способствующих распространению преступлений экстремистского и террористического характера, предупреждением и пресечением действий, экстремистских и террористических организаций, противодействие распространению идеологической составляющей терроризма и информационно-пропагандистского обеспечения, а также проведение антитеррористических мероприятий.

Для наиболее эффективного противодействия террористической и экстремистской деятельности в открытых интернет источниках, необходима

своевременная разработка и принятие исчерпывающего комплекса мер, направленного на осуществление оперативно-розыскного, профилактического и пропагандистского характера.

Целью экстремизма является:

1. Насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации;

2. Публичное оправдание терроризма и иная террористическая деятельность;

3. Возбуждение социальной, расовой, национальной или религиозной розни;

4. Пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

5. Нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

6. Воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

7. Воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

8. Пропагандистское воздействие на сознание людей и дезинформирование;

9. Совершение террористических актов, диверсий на различных объектах инфраструктуры, социальной сферы и транспорта.

В последние годы, транспортно-логистическая система России, является одной из самой приоритетной и активно развивающейся отраслью. С каждый годом, (в зависимости от региона) повышается пассажиропоток и оборот грузоперевозок, проходит плановую модернизацию и расширяется инфраструктура объектов транспорта, развивается сеть железнодорожных путей сообщения, строятся новые ж.д. станции, автомобильные дороги и магистрали, воздушные терминалы и т.д. По данным объектам транспорта, постоянно перемещается большое количество горюче-смазочных материалов, химических веществ и других материалов, на которые нацелены террористические и экстремистские организации, криминальные элементы и диверсионно-разведывательные группы (ДРГ).

С учетом складывающейся в Российской Федерации социально-политической обстановки, объекты и вся в целом транспортная инфраструктура находятся в зоне повышенного риска и высокой уязвимости от действий противозаконного вмешательства, прежде всего это связано с террористическими актами, направленными на создание, как общественного резонанса, так и причинение значительного ущерба государству, организациям

и обществу. Выявление и пресечение угроз совершения актов противозаконного вмешательства в деятельность транспортной инфраструктуры, в большей степени ложится на плечи сотрудников ОВД на транспорте, совместно с подразделениями ФСБ России, которые анализируют и разрабатывают наиболее эффективные методы антитеррористической и противодиверсионной защищенности объектов транспорта.

Еще из приоритетных направлений ОВД на транспорте, является сопровождение пассажирских, пригородных поездов и прогулочных пассажирских судов, отработка пассажиропотока на железнодорожных вокзалах, автовокзалах и аэропортах, на предмет выявления лиц, которые могут быть причастны к экстремистской и террористической деятельности, а также выявление и пресечение преступлений и административных правонарушений.

Литература

1.Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

2. Ганаев Е.Э. «Молодежный экстремизм, как тип девиации» Молодой ученый - 2012.

3. Инструкция об организации взаимодействия территориальных органов МВД России на железнодорожном, водном и воздушном транспорте с иными территориальными органами МВД России: приложение № 1 к приказу МВД России от 28 марта 2015 г. № 381.

4. Снайдер С. Протоколы «Интернета вещей»: основные сведения / Мир компьютерной автоматизации: встраиваемые компьютерные системы. 2015.

Самуйленко Федор Петрович,
старший преподаватель
Краснодарского университета МВД России

Самуйленко Людмила Викторовна,
преподаватель
Волгоградской академии МВД России

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

На современном этапе развития информационных и телекоммуникационных технологий, таких как интернет, социальные сети и другие коммуникационные приложения, которые плотно проникли во все сферы деятельности человека и стали неотъемлемой частью его образа жизни, растет и возможность влияния данных ресурсов на мышление, принимаемые решения и поведения людей. В силу объективных причин воздействие электронной среды в большей степени охватывает молодые слои населения[1]. При этом необходимо отметить, что отдельные группы людей и более старшего возраста являются активными пользователями различных электронных ресурсов.

Отмечая положительные стороны глобального распространения информационно-телекоммуникационных технологий в повседневной жизни людей, нельзя не затронуть и возможность их использования в приступных целях. К сожалению, статистика показывает, что современные технологии активно используются преступниками по самым различным направлениям. Примером могут служить как различного рода мошеннические схемы, вымогательство, шантаж, так и преступления экстремистского и террористического характера.

Согласно статистике в январе – феврале 2024 года сохраняется тенденция роста числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Прирост количества преступлений составил 23,5% по сравнению с аналогичным периодом 2023 г. Об этом сообщает Министерства внутренних дел России.

Использование современных технологий в преступных целях позволяет злоумышленникам охватить очень широкий круг граждан в достаточно

---

[1] Кочубей М.А., Мареев П.Л. Профилактика терроризма и экстремизма в молодежной среде. – СПб.: ООО «Издательство «Русь», 2018. – 96 с.

короткий промежуток времени, при этом, самим оставаясь дистанцированными[1]. При этом не все группы граждан, попадая под преступное влияние, могут объективно оценивать угрозу манипулирования ими. Что влечет к опасным последствиям, как для человека, так и для государства в целом.

Одним из самых опасных направлений использования ИКТ в преступных целях, является их применение в экстремисткой и террористической деятельности. Борьба правоохранительных органов с данными проявлениями лежит в основе безопасности страны.

Чтобы активно противостоять угрозам экстремистского и террористического характера, надо подробно разобраться, как устроен преступный алгоритм работы. Анализируя имеющуюся информацию и опыт работы практических органов можно выделить следующие этапа преступной работы:

- Психологическая обработка.
- Организация пропаганды
- Осуществление вербовки
- Радикализация
- Организация финансирования
- Обучение и тренировка
- Кибератаки.

Психологическая обработка – направлена на формирования у пользователя ложного ощущения несправедливости по отношению к нему. Критическое восприятие любых действия государственных органов. Создание подменных идеалов. Формирование чрезмерной чувствительности к событиям происходящим в мире, с акцентированием аспектов в своих целях. В большей степени данной психологической обработке подвержена молодежь. Играя на неокрепшей психики стараются пробудить агрессию ко всему происходящему. При этом осуществляются призывы примкнуть в свои ряды.

Организация пропаганды – в основе пропагандистской деятельности экстремистских организаций лежит привлечение сторонников для вербовки, радикализация и подстрекательство к террористическим действиям. В качестве наглядных инструментов применяются видеоролики насильственных актов, боевых действий, выступления лидеров запрещенных организаций. Так же могут распространятся характерные видеоигры, отчеты мероприятий.

Осуществление вербовки – работа, направленная на формирование отношений с наиболее отзывчивыми. Используются при этом защищенные сайты и группы с ограниченным доступом в интернет-чатах. Необходимо отметить один из наиболее распространенных способов вербовки через различные социальные сети.

Радикализация – процесс регулярной идеологической обработки сотрудников.

---

[1] Опалев А. В. Современные информационные технологии как инструмент деятельности экстремистских и террористических организаций // Вестник Московского университета МВД России. 2022. № 5. С. 187–190. https://doi.org/ 10.24412/2073-0454-2022-5-187-190.

Организация финансирования – активно применяются возможности интернета для сбора средств. Можно отметить активизацию деятельности в чат-группы, применение массовых рассылок, создание дублеров известных интернет магазинов. Осуществляются попытки проникновения к финансам различных благотворительных организаций.

Обучение и тренировка – используя интернет платформы распространяются практические руководства, онлайн пособия, видеоклипы и различные рекомендации. Фактически формируется виртуальный лагерь, позволяющий организовать отработку действий, обмен информацией, осуществлять планирование и разработку террористических актов.

Кибератаки – организация деятельности, направленная на преднамеренное нарушение штатной работы компьютерных систем, серверов и площадок различных органов путем взлома, распространения компьютерных вирусов или вредоносного ПО.

Анализ алгоритма действий экстремистских и террористических ячеек в своей деятельности с применением информационно-телекоммуникационных технологий позволяет структурировать работу правоохранительных органов. Способствует правильной организации работы подразделений по борьбе с экстремизмом и терроризмом на этапах подготовки к совершению преступления. Пресекать источники финансирования. Отслеживать активных участников и потенциальных новобранцев.

Одним из важных аспектов по предотвращению террористических актов является конструктивное сотрудничество средств массовой информации, органов власти и правопорядка. Освещение событий не должно работать на террористов. Журналисты однозначно обязаны поддерживать действия властей при осуществлении контртеррористических операций и по их требованию распространять информацию от имени государства. В этой связи, работа соответствующих государственных структур должна быть направлена на то, чтобы СМИ заклеймили террористов в глазах общественности как преступников (прежде всего путем предоставления средствами массовой информации материалов о преступной деятельности террористов и созданных ими организаций).

Литература

1. Опалев А. В. Современные информационные технологии как инструмент деятельности экстремистских и террористических организаций // Вестник Московского университета МВД России. 2022. № 5. С. 187–190. https://doi.org/ 10.24412/2073-0454-2022-5-187-190.

2. Кочубей М.А., Мареев П.Л. Профилактика терроризма и экстремизма в молодежной среде. – СПб.: ООО «Издательство «Русь», 2018. – 96 с.

Столбоушкина Татьяна Анатольевна,
преподаватель кафедры судебно-экспертной деятельности
Краснодарского университета МВД России

Столбоушкин Вадим Алексеевич,
студент Кубанского государственного
технологического университета

АНАЛИЗ ПОНЯТИЯ «КИБЕРСТАЛКИНГ»

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационно-телекоммуникационные технологии, компьютеры и компьютерные сети в целях достижения материальной или иной выгоды. С помощью кибертехнологий мошенники могут получить практически любую информацию о субъекте, которую в дальнейшем направят против самого субъекта. Обеспечить полную безопасность в информационной сфере не удается возможным, так как человек всегда будет являться самым слабым звеном в этой большой цепи. С каждым годом жертв, пострадавших от киберпреступников становится все больше и больше. Две трети утечек информации происходят не в силу злого умысла, в остальных случаях это намеренные действия киберпреступников, сотрудников организации или ее подрядчиков.

Согласно отчету специалистов Positive Technologies за II квартал 2019 года, целенаправленные атаки преобладают над массовыми. Более половины всех киберпреступлений совершаются с целью кражи информации. Персональные данные — основной тип украденной информации в атаках на юридические лица. Частные лица наиболее часто рискуют учетными записями и данными своих банковских карт.

Понятие «Кибersталкинг» пришло в общественное пространство совсем недавно. Вместе с развитием информационных технологий, развиваются и способы времяпрепровождения обычного пользователя в сети «Интернет». Таким способом преступники начали находить новые лазейки, с целью получения материальной выгоды. Спустя время появилась определенная прослойка кибермошенников, называющих себя «Кибersталкерами». Кибersталкинг — это цифровая атака на человека, который был выбран жертвой по причине ненависти, мести или желания манипулировать [1]. Кибersталкинг может принимать множество форм, в том числе:

1. Домогательство и унижение жертвы.
2. Воровство с банковских счетов или других финансовых носителей.
3. Домогательство семьи, друзей или сотрудников ради изолирования жертвы.
4. Тактика запугивания.

Кибersталкер – лицо (практически всегда анонимное), осуществляющее «Кибersталкинг», целью которого является стремление запугать

жертву, подорвать ее психику и нарушить нормальную дееспособность путем использования цифровых устройств, а также сети «Интернет» [2].

Мотивы таких людей могут быть различны: начиная с простого привлечения внимания и заканчивая желанием получить материальную выгоду с жертвы. Опираясь на данные из интернета, кибersталкеров можно подразделить на несколько основных типов:

1. «Отверженные». Данный тип характеризуется тем, что кибersталкер преследует бывших друзей или знакомых, в надежде отомстить за полученную в давнем времени моральную травму.

2. «Несостоятельные поклонники». Эта разновидность кибersталкеров чаще всего выражается в неправомерном навязывании себя тому или иному человеку, чтобы добиться внимания. Зачастую такие злоумышленники надеются на короткий интимный контакт или свидание.

3. «Сталкеры-хищники». Характеризуются тем, что преследуют жертву ради получения не только моральной компенсации, но и материальной. Такой вид не останавливается на достижении единоразового результата. Зачастую преступник будет преследовать жертву, вплоть до ее жизненного конца, либо пока не найдет более «привлекательную» цель.

С развитием информационных технологий развиваются и новые способы получения личной информации о пользователе – краже его электронной личности. Однако, опираясь на актуальную информацию, на сегодняшний день можно выделить несколько тактик, которые чаще всего используют кибersталкеры:

1. Взятие под контроль онлайн-аккаунтов жертв на разных пользовательских сайтах или форумах, запрашивающих при регистрации вашу персональную информацию.

2. Отслеживание жертв с помощью мобильного GPS или шпионского ПО на телефонах. Данная тактика встречается реже всего.

3. Создание фальшивого профиля жертвы в известных социальных сетях и мессенджерах (Вконтакте, Одноклассники, Instagram).

4. Отправление прямых угроз убийства через электронную почту или мгновенные сообщения.

4.1. Преследование цели или преследование родственников жертвы, друзей с угрозами ему.

5. Размещение изображений жертв на порнографических сайтах (запрещенных на территории РФ).

6. Использование анонимных номеров. Вследствие звонков на мобильное устройство жертвы.

Даркнет (англ. *DarkNet*, также известен как «Скрытая сеть», «Темный интернет», «Тёмная сеть», «Теневая сеть», «Тёмный веб») — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. [3]. Ресурсы для анонимного пользовательского общения всегда были привлекательными, как для людей, которые не хотели выдавать

свою настоящую личность, так и для мошенников, которые знали, что за содеянное преступление они не понесут никакой ответственности. Стоит сказать, что основные ресурсы в Даркнете — это всевозможные магазины и форумы с нелегальной информацией, а значит, этот сегмент интернета является идеальным местом для кибersталкеров, так как те, могут получать денежную компенсацию за проделанную работу. В данном случае анонимность скрытых сетей позволяет им действовать более эффективно.

На сегодняшний день существует множество примеров инцидентов с кражей личных данных и продажей их в темной сети DarkNet. С каждым разом преступников становится все больше, так как данный вид заработка становится простым и открывает для тебя множество дверей – дверей в противоправный мир.

В Российской Федерации не предусмотрена какая-либо ответственность за деятельность, связанную с травлей. Однако существует ряд составов в административном и уголовном законодательстве, предусматривающих наказание за отдельные виды посягательств на личность.

Для борьбы с «Кибersталкингом» необходимо предпринять некоторые меры. Первым делом начать следует с защиты своих данных, обратить внимание на ваши страницы в социальных сетях, удалить личные данные, которые вы не размещали, опаской относиться к любым просьбам сообщить личные данные в письме или по телефону, как бы разумно они ни звучали. Также ни в коем случае не стоит забывать о безопасности вашего персонального компьютера или мобильного устройства. Подводя итог вышесказанному следует отметить, что кибersталкинг – новое понятие в среде информационных технологий. Аналогично и с определением теневой сети DarkNet. В данной статье было подробно расшифровано значение данных терминов, а также установлена связь между ними. Стоит сказать, что на сегодняшний день данные понятия все чаще употребляются не по отдельности, а в совокупности. Вследствие чего количество жертв кибersталкинга преумножается в разы. Данная тема не потеряет своей актуальности спустя долгие годы, так как с развитием информационных технологий увеличивается и количество способов использования их в незаконных целях. На данный момент человек каждый день сталкивается с риском стать жертвой кибersталкеров. Самым страшным является тот факт, что никто не сможет с полной уверенностью сказать, что он защищен от киберпреступников и их атак. Стоит помнить, что в случае, если кибersталкер целенаправленно захочет заполучить ваши данные, помимо личного контакта с вами, он попытается взломать всевозможные базы данных, в которых вы были так или иначе упомянуты. Именно поэтому тема «Кибersталкинга» является важной для каждого из нас и любой беспокоящийся за себя пользователь обязан полностью ознакомиться с ней.

Литература

1. Кибersталкинг как новый вид уголовно-наказуемого деяния Барышева К.А. Союз криминалистов и криминологов. 2017. № 1-4. С. 63-66.

2. Кибersталкинг как угроза безопасности современного общества Бессчетнова А.А. В книге: Здоровье как ресурс: V. 2.0. Международная научно-практическая конференция. Под общей редакцией З.Х. Саралиевой. 2019. С. 212-214.

3. Клейманов М.С. Проблема криминализации сталкинга в Российской Федерации. Закон и право. 2021. № 5. С. 133-135.

4. О понятии «киберпреступность» Таганов С.А. В сборнике: Молодость. Интеллект. Инициатива. Материалы VIII Международной научно- практической конференции студентов и магистрантов. 2020. С. 353-354.

Фаниев Павел Андреевич,
эксперт организационно-методического отдела
ЭКЦ ГУ МВД России по Краснодарскому краю

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ «ТРОЯНСКОГО» ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ ПРЕСТУПНИКА

Если мы оглянемся назад и внимательно изучим историю полиции, то столкнемся с интересным фактом, говорящим не в пользу силовых структур. Парадоксально, но передовые технологии в первую очередь эффективно использовались преступниками, нежели правоохранительными органами. Например, в конце XIX века, полиция Чикаго использовала в качестве транспорта гужевой транспорт, преступники уже в полной мере использовали автомобили. Первые модели шестизарядных револьверов были использованы именно преступниками, а уже потом поступали на вооружение в правоохранительные органы. Когда в России морально устаревший «Смит Вессон» был заменён на наган, излюбленным оружием террористов был браунинг.

Мобильный телефон активно использовались наркоторговцами для координации преступной деятельности задолго до того, как они нашли свое применение в полиции. Аналогичная тенденция складывается и в наши дни. Сегодня, с учетом стремительного роста высоких технологий, арсенал преступников стремительно расширяется. Особенно это касается киберпреступлений. Широкий ассортимент вирусного программного обеспечения (далее – ПО), перехватчики и дешифраторы цифрового сигнала, различные sim-боксы – все это стало постоянным спутником современного киберпреступника. При этом, не смотря на наличие технических возможностей и открывающиеся новые пути расследования преступлений, ряд инструментария злоумышленников, так и не был поставлен на вооружение правоохранительных органов. Одним из ярких примеров подобного орудия являются программы категории Remote Access Trojan (трояны удаленного доступа), получившие сленговое название «ратник». Глобально, основной принцип их работы схож с таким ПО как RAdmin, AnyDesk, TeamViewer и многие другие. Однако имеется одно ключевое отличие. Весь вышеперечисленный софт так или иначе уведомляет пользователя о факте своего присутствия и эксплуатации. Например, TeamViewer – при первом запуске предложит случайную пару из уникального ID и случайно сгенерированного пароля, для установки AnyDesk потребуются права администратора, а в случае с RAdmin – для первого запуска потребуется физическое нахождение перед атакуемым устройством. С «ратниками» - дело обстоит иначе. Поскольку для генерации файлов, данная категория ПО использует наработки вирусных троянских программ, для заражения требуется единожды запустить их на атакуемом устройстве. После этого программа включиться в фоновом режиме, никак не выдавая свое присутствие. Это позволяет осуществлять изучение в режиме

online мониторинг за деятельностью преступника, осуществлять фото и видео запись происходящего на его рабочем столе, копировать необходимые данные, блокировать доступ к устройству в целях обеспечения сохранности цифровых следов в случаях задержания злоумышленника и многое другое. Однако их использование имеет ряд особенностей как правового, так и технического характера. Давайте рассмотрим оба этих аспекта независимо друг от друга.

Использование подобного рода ПО возможно для проведения таких оперативно-розыскных мероприятий как контроль почтовых отправлений, телеграфных и иных сообщений, снятие информации с технических каналов связи, а также получение компьютерной информации. При этом, напрямую затрагивается одно из основных прав и свобод человека и гражданина, а именно право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, гарантированное статьей 23 Конституции Российской Федерации. Согласно которой, ограничение этого права допускается только на основании судебного решения. Следует отметить, что уже имеется практика применения подобного ПО в странах Европейского Союза, которые принимают определённые меры реагирования. Например, ввиду часто поступающих жалоб в Федеральный Конституционный суд Германии привели к изменению в уголовно-процессуальном кодексе, разрешающие использование так называемых «Государственных троянцев»[1]. Законодательство Испании не содержит положений, касающихся использования вирусного ПО, при этом полицией активно используются различные программы подобного типа. Данный пробел отчасти восполняется практикой Верховного суда Испании, который указал на то, что использование данных программ не требует судебного ордера, а доказательства, полученные таким образом, являются допустимыми[2]. Кроме того, использование «троянского» ПО, требует от сотрудника определенных познаний в области системного администрирования, поэтому видится целесообразным привлекать для проведения подобных ОРМ специалистов, обладающих специальными познаниями в вышеуказанной области.

Техническая составляющей тоже имеет ряд особенностей:

---

[1] Verfassungsbeschwerden von unter anderem Rechtsanwälten, Künstlern und Journalisten, darunter einige Mitglieder des Deutschen Bundestages, zu der Frage, ob die durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202, in Kraft getreten am 24. August 2017) bewirkten Änderungen der Strafprozessordnung (StPO), insbesondere die Möglichkeit der Anordnung der sog. Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung (mittels des sog. „Staatstrojaners“), verfassungsgemäß sind. URL: https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2021/vorausschau_2021.html

[2] Уголовно-процессуальный киберпанк: компьютерные вирусы на службе правосудия. URL: https://zakon.ru/blog/2018/10/14/ugolovno-processualnyj_kiberpank_kompyuternye_virusy_na_sluzhbe_pravosudiya

1) Работа с «троянским» ПО может быть сопряжена с риском заражения используемого устройства. Это связано с тем, что большинство программ для создания «ратников» изначально создавались «black hat» - хакерскими сообществами, и как правило могут быть заражены вирусом, зачастую майнером. Ввиду этого, рекомендуется производить любые действия по скачиванию и эксплуатации подобного ПО только в виртуальной машине.

2) Учитывая специфику работы программ этой категории, подавляющее большинство антивирусных программ будут определять в качестве вируса сам «ратник», и поэтому обязательным условием их использования является отключение антивирусной защиты и брандмауэра.

3) Использование публичного «белого» IP-адреса и открытие портов – для реализации своих функций «ратнику» необходимо использовать публичный IP-адрес родительского устройства, а также один из открытых портов соединения с Интернетом. При этом, в случае если преступник обладает должной квалификацией, он сможет получить эти данные, там самым разоблачив направленные против него действия. Ввиду этого, в целях снижения риска своей деанонимизации рекомендуется использовать VPN.

Опираясь на вышесказанное, можно предложить следующий алгоритм использования троянского ПО:

1) Создайте виртуальную машину под управлением ОС Windows. Для этого возможно использовать специализированное программное обеспечение. Наибольшей популярностью пользуются программы VirtualBox, Hyper–V и VMware Workstation. Каждая из них имеет свои преимущества и недостатки, в нашем случае, мы будем использовать VirtualBox. Для этого есть ряд причин. Во-первых, поскольку VirtualBox распространяется по лицензии GNU (General Public License), пользователь получает возможность использовать весь её функционал. Во-вторых, функциональная возможность создания моментальных «снимков» (snapshot) операционной системы, используя которые можно восстановить данные в случае их уничтожения. В-третьих, кроссплатформенность VirtualBox, позволяет установить его на любую из наиболее распространённых операционных систем.

2) Установите VPN соединение и откройте один из портов для протоколов TCP и UDP. Использование которых обусловлено не только особенностями работы «ратника», но и необходимостью наиболее оптимального распределения трафика как при скачивании данных, так и при просмотре потокового видео.

3) Скачайте любое доступное ПО для создания «троянских» программ из репозиториев GitHub. Скачивание программы с других интернет ресурсов не рекомендуется поскольку велик риск получить зараженное ПО. Дальнейший анализ «ратника» осуществлялся на базе программы NjRat 0.7D Danger Edition, скачанной с GitHub репозитория пользователя M6YR по ссылке https://github.com/M6YR/NjRat-0.7D-Danger-Edition-Cracked-By-MMLo7.

4) Создайте вирусное ПО. Для этого необходим запустить скачанную программу. В первом появившемся окне необходимо указать открытый нами

порт. Затем в появившемся окне необходимо нажать кнопку «Builder». Появится окно конфигурации «ратника». В строке Host- DNS Address указать используемый IP-адрес и нажать «Added». Это необходимо для включения шифровки host-адреса. Затем, необходимо выбрать все остальные, необходимые нам параметры. Примечательно, что NjRat обладает достаточно высокими возможностями в конфигурировании создаваемого вируса. Давайте рассмотрим некоторые вариантов:

№	Параметр.	Значение.
Раздел Stting Paylod.		
1	Scheduled Tasks	Включение «ратника» в планировщик задач.
2	Hide Server	Сокрытие группы процессов серверной части вируса.
3	Not Kill Server	Блокировка возможности отключения процесса.
4	Masg Box	При запуске вируса, появляется сообщение об ошибке.
5	Protect Process (BSOD)	В случае закрытия процесса, появляется ошибка BSOD (синий экран смерти).
6	Excluir Arquivo (Meit)	Удалить вирусный файл, после его интеграции в устройство.
7	Delete archives	Удалить архивы и логи работы.
8	Bypass Firewall Windows	Получение прав администратора для управления Firewall.
9	DisableTaskMgr	Блокировка диспетчера задач после запуска вируса.
10	USB Spread	Распространение вируса через USB.
11	Kill Anti Process	Блокировать и удалят противостоящие антивирусные процессы.
Раздел Instal/Director		
1	Copy StartUp	Копирование «ратника» в автозагрузку.
2	Spread Disco Local	Распространение по локальным дискам.
3	Spread Hard Desk	Распространение по жестким дискам.
4	Registy StarUp	Внедрение в реестр.
5	Directory	Копирование в определенную директорию.
6	Copy Directory	Копировать в директорию из списка.

После определения всех необходимых настроек, нажать кнопку «Build», присвоить имя файла и сохранить вирус.

5) Замаскируйте вирус. С одной стороны, после завершения этапа 4 у нас уже имеется полноценное троянское ПО для внедрения. С другой, шансов на то, что вирус в подобном виде будет добровольно активирован пользователем мало. Ввиду этого, необходимо провести его дополнительную маскировку. Тут возможны несколько подходов. Во-первых, можно прове-

сти обфускацию – запутывание исходного кода файла, без потери его функциональности для усложнения его анализа антивирусным ПО. Для этого можно использовать либо специализированные программы, либо сторонние онлайн ресурсы, например, freeobfuscator.com. Во-вторых, желательно произвести шифрование вируса. Тут можно использовать любой доступный шифровальщик, как онлайн, так и офлайн. В-третьих, маскировка «ратника» под легальный файл. Этого можно достичь различными способами, однако наибольшее распространение получили алгоритмы стеганографии или специальное ПО для объединения файлов, на базе шестнадцатеричных редакторов данных, например, HxD – Freeware Hex Editor and Disk Editor (https://mh-nexus.de/en/hxd/). С их помощью можно спрятать вирус в графическое изображение, либо в pdf документ. После осуществления всех действий по защите «ратника», необходимо обеспечить едино разовый запуск полученного файла на компьютере злоумышленника, что позволит нам осуществлять мониторинг и фото-видео съемку за его деятельностью на зараженном устройстве. Передача зараженного файла также может осуществляться любым доступным способом, например, по средствам мессенджеров и облачных хранилищ.

Уважаемые коллеги, в заключение хочу ещё раз обратить ваше внимание, что использование «троянского» ПО в правоохранительной деятельности дает большие возможности для раскрытия преступлений и расследования уголовных дел. Мониторинг за деятельностью преступника может способствовать не только качественному сбору доказательственной базы и цифровых следов, но и оказать неоценимую помощь в деле профилактирования и предупреждения преступлений на начальном этапе. При этом следует помнить, что применение подобных методов без судебной санкции недопустимую.

Литература

1. Конституция Российской Федерации URL: https://www.consultant.ru/document/cons_doc_LAW_28399/

2. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_7519/

3. Разъяснение федерального конституционного суда Германии. Второй сенат. Докладчик BVR Dr. Maidowsk URL: URL: https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2021/vorausschau_2021.html

4. Статья: Уголовно-процессуальный киберпанк: компьютерные вирусы на службе правосудия. URL: https://zakon.ru/blog/2018/10/14/ugolovno-processualnyj_kiberpank_kompyuternye_virusy_na_sluzhbe_pravosudiya

Цыцурин Сергей Леонидович,
старший научный сотрудник Центра средств и систем связи
ФКУ НПО «СТиС» МВД России

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС АНАЛИЗА И РАСПОЗНАВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Технология биометрической идентификации человека базируется на алгоритмах распознавания и сравнения изображений, основанных на ансамбле искусственных нейронных сетей, обрабатывающих изображения лица человека.

Рассматриваемый Комплекс представляет собой комплект технических средств, в который входит автоматизированное рабочее место с установленным на нём клиентским приложением, через интерфейс которого пользователь взаимодействует с центральным индексным сервером FindFace, имеющим соответствующее программное обеспечение виртуализации
и системного окружения.

Индексный сервер, в свою очередь, подготавливает исходные данные по изображению лица человека, передаваемого от клиентской части, а также обрабатывает результаты поиска информации.

Комплекс эксплуатируется в сетевом многопользовательском режиме с предоставлением доступа неограниченному числу пользователей
с клиентских рабочих мест, выполняя три основные функции:

формирование, сопровождение и хранение базы данных, включающей в себя массив сведений биометрического характера об объектах заинтересованности;

автоматическое извлечение биометрических данных из фотоизображения объекта интереса;

отождествление интересующего лица путём сопоставления с массивом биометрической базы данных индексного сервера.

Изготовителем, в зависимости от максимального размера биометрической базы данных и количества одновременно параллельно обрабатываемых потоков цифровых видеоданных, предусмотрены 8 конфигураций Комплекса.

Минимальная конфигурации содержит биометрическую базу данных размером не более 1000000 изображений, с возможностью одновременной параллельной обработкой не более 5 единиц цифровых потоков видеоданных.

Максимальная конфигурации предусматривает биометрическую базу данных неограниченного размера с возможностью одновременной параллельной обработки не более 200 единиц цифровых потоков видеоданных.

Формирование и сопровождение биометрической базы данных физических лиц индексного сервера обеспечивается путём выполнения следующих функций:

первоначального наполнения и его систематического обновления путём импорта данных полученных по сети Интернет, а также из смежных информационных систем-источников заказчика с помощью сервисных программ-адаптеров;

автоматизированной обработки фото и видеоматериалов (видеофайлов) путём детектирования в них изображения лица человека с автоматическим занесением их в массив данных;

возможность добавления к каждой хранимой единице данных сведений биометрического и не биометрического характера (метаданных), относящихся
к описанию индивида.

Таким образом, Комплекс позволяет автоматически:

обрабатывать фотографии, загружаемые пользователем в программу, с распознаванием на них изображения лица человека и извлечения из него биометрического признака (шаблона);

формировать индексный сервер массива данных;

передавать извлечённый биометрический признак в индексный сервер для поиска в нём данных и формирования результирующего массива;

проводить биометрический мониторинг путём сопоставления биометрического шаблона с множеством биометрических шаблонов, хранимым в массиве биометрической базы данных;

отслеживать детектированный биометрический образец в кадрах цифрового потока видеоданных, принимаемых от видеокамеры или считываемых из видеофайла (видеоархива), с автоматическим выбором наилучшего кадра, за счёт максимальной для данного биометрического образца интегральной оценки качества;

определять дополнительные признаки изображения лица, такие как пол, возраст, эмоциональное выражение, наличие бороды, очков
с разделением на солнцезащитные и для коррекции зрения, а также
медицинской маски, с разделением на правильно и неправильно надетую;

обрабатывать результирующий массив, принятый от индексного сервера, с выводом на пользовательский интерфейс данных об адресах страниц пользователей сети Интернет, схожих с искомым образцом, а также сами изображения;

предоставлять пользователю возможность визуального анализа результирующего массива, в том числе путём перехода по ссылкам на страницы пользователей сети Интернет, связанных с обнаруженными изображениями, с последующим выбором пользователем определённого биометрического образца, распознанного на исходном изображении. Выбор может происходить автоматически, если распознан единственный биометрический образец.

Комплекс может осуществлять двустороннее взаимодействие со смежными биометрическими системами, входящими в состав правоохранительного сегмента АПК «Безопасный город», а также других поисковых систем.

Комплекс обеспечивает биометрическую идентификацию индивида за счёт передачи биометрического признака в смежную биометрическую информационную систему с помощью подключаемого модуля обмена данными FindFace DEM SE.

Функции импорта данных в массив биометрической базы данных Комплекса из информационных систем-источников реализуется за счёт сервисных программ-адаптеров, входящих в состав Комплекса.

При использовании данного универсального шлюза обмена данными возможно установление регулярного местонахождения объектов оперативной заинтересованности, их привычных маршрутов перемещения, определение социальных связей, контактов ближнего круга общения.

При необходимости импорта данных из иных информационных систем-источников соответствующие сервисные программы-адаптеры могут быть разработаны изготовителем или самостоятельно заказчиком с использованием интерфейса прикладного программирования Комплекса.

К обрабатываемым Комплексом цифровым фотографическим изображениям, а также в отношении детектирования биометрического образца при обработке потоков цифровых видеоданных к изображению лица в кадре предъявляются следующие требования:

формат файла - JPEG, PNG;

размер - не более 5 Мбайт и 20 мегапикселей;

количество детектируемых на одном изображении биометрических образцов - без ограничений;

отклонение от фронтального ракурса в вертикальной плоскости - не более 90°, во фронтальной плоскости - не более 45°, в горизонтальной плоскости - не более 30°;

неоднородность фона - 0,2 – 0,8;

освещённость в плоскости лица – 100 - 1000 лк;

неравномерность освещённости лица – 50 %;

размер детектируемого образца по горизонтали - не менее 60 пикселей;

динамический диапазон интенсивности детектируемого образа - не менее 8 бит;

перекрытие площади детектируемого образца - не более 40 %.

К обрабатываемым Комплексом цифровым видеоизображениям и их характеристикам предъявляются следующие требования и ограничения:

формат сжатия видеоданных - H.264, H.265, MJPEG;

протоколы передачи видеоданных в режиме прямой трансляции RTSP, HTTP;

тип медиаконтейнера видеофайла - AVI, MKV, MOV, MP4;

минимальное разрешение видеопотока - 720×576 пикселей;

максимальное разрешение видеопотока - 3840×2160 пикселей;

минимальная частота кадров в секунду – 15;

максимальная частота кадров в секунду– 30.

Комплекс допускает обработку изображений, имеющих отклонения от указанного типа изображения лица, однако следует принимать во внимание, что результаты обработки (в частности, биометрического поиска) могут ухудшаться.

Допускается также отказ от обработки изображения, если лица находятся не в фокусе, сильно размыты, подвергнуты цифровому редактированию (ретуши) или в значительной части своей площади перекрыты (элементами маскировки, предметами одежды, посторонними объектами и др.).

Требования к составу и конфигурации технических средств Комплекса определяются следующими параметрами:

максимальный размер биометрической базы данных;

количество одновременно параллельно обрабатываемых потоков цифровых видеоданных;

количество пользователей, работающих с интерфейсом Комплекса в конкурентном режиме;

количество смежных информационных систем, обращающихся к интерфейсу прикладного программирования Комплекса в конкурентном режиме;

количество запросов в единицу времени.

Для корректной эксплуатации Комплекса в качестве АРМ пользователя используется персональная ЭВМ под управлением операционной системы Linux, Apple MacOS, Microsoft Windows, поддерживающих корректную стабильную работу таких веб-браузеров как: Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox, Яндекс Браузер.

Комплекс предназначен для эксплуатирования в непрерывном круглосуточном режиме с организацией регламентных перерывов для проведения профилактического и технического обслуживания.

Частикова Вера Аркадьевна,
кандидат технических наук,
доцент Кубанского государственного
технологического университета

Меркулов Павел Алексеевич,
студент Кубанского государственного
технологического университета

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ VULNERABILITY MANAGEMENT

Введение

В современном цифровом мире безопасность информации становится все более важной и приоритетной задачей для организаций. Управление уязвимостями играет ключевую роль в обеспечении защиты от киберугроз и минимизации возможных угроз для информационных систем.

В данной статье рассматриваются актуальные тенденции и подходы к управлению уязвимостями, основные аспекты эффективного подхода к обнаружению и классификации уязвимостей, а также передовые технологии, такие как: искусственный интеллект и машинное обучение, для улучшения кибербезопасности.

В работе описывается важность управления уязвимостями в условиях постоянно меняющейся среды угроз и предлагаются рекомендации для обеспечения информационной безопасности.

Важность управления уязвимостями

Управление уязвимостями (англ. Vulnerability Management) — это основанный на оценке рисков подход к кибербезопасности, с помощью которого организации активно защищают свою цифровую инфраструктуру от взломов. Он включает в себя идентификацию, оценку и устранение уязвимостей безопасности в компьютерных системах, приложениях и сетях с целью предотвращения кибератак и ограничения потенциального ущерба в случае их возникновения [1].

В условиях участившихся киберугроз и обнаружения тысяч уязвимостей ежедневно, организации вынуждены активно заниматься ими с целью определения их степени серьезности и в дальнейшем оперативного устранения. Только путем непрерывного выявления, классификации и устранений угроз организации смогут обеспечить эффективную защиту от потенциальных кибератак.

В 2020 году компании сообщили в общей сложности о 18 103 уязвимостях в 2020 году [2] – самом высоком количестве, когда-либо зарегистрированных за один год, - в среднем по 50 в день, согласно Национальному институту стандартов и технологий и его Национальной базе уязвимостей.

Пятьдесят семь процентов (10 342) уязвимостей в 2020 году были классифицированы как критические или высокой степени серьезности, что больше, чем общее количество уязвимостей, зарегистрированных в 2010 году (4639).

В условиях динамичного ландшафта угроз важно развивать стратегии управления уязвимостями. Положительной тенденцией является внедрение инновационных методов, что обещает улучшение безопасности в будущем.

Основные факторы, определяющие работу с уязвимостями

Совместный обмен информацией об угрозах. Организации все чаще обмениваются информацией о потенциальных кибератаках друг с другом, чтобы лучше подготовиться и защитить себя. Они могут усилить свою защиту от этих угроз.

Акцент на мобильную безопасность. Мобильная безопасность приобретает все большее значение, поскольку компании все больше полагаются на мобильные устройства. Для решения этой проблемы организации предпринимают шаги по обеспечению безопасности мобильных приложений, устройств и сетей, учитывая уникальные вызовы и угрозы в мобильной экосистеме.

Внедрение приоритизации на основе рисков. До недавнего времени, когда дело касалось кибербезопасности, большинство организаций старались как можно быстрее устранить каждую обнаруженную уязвимость. Однако, вместо этого, все можно делать более практично и эффективно.

Основное внимание уделяется выявлению и приоритизации угроз безопасности, которые представляют значительный риск для организации. Это означает рассмотрение таких вещей, как: вероятность возникновения конкретной угрозы, насколько серьезными могут быть последствия и сколько усилий требуется для ее устранения.

Интеграция искусственного интеллекта и машинного обучения

Автоматизация процесса управления уязвимостями становится одной из главных целей современной кибербезопасности [3]. Искусственный интеллект (ИИ) и машинное обучение (МО) все чаще интегрируются в решения по управлению уязвимостями для прогнозирования и выявления возникающих угроз. Эти технологии могут анализировать исторические данные и текущие тенденции, чтобы предвидеть, где могут возникнуть уязвимости, что позволяет организациям активно устранять потенциальные слабые места до того, как они будут использованы.

Расширение охвата устройств IoT

Распространение устройств Интернета вещей (IoT) расширило зону атак для многих организаций. Решения по управлению уязвимостями теперь включает в себя более комплексные инструменты, специально разработанные для решения уникальных проблем, связанных с IoT, например, таких как частые обновления прошивки [4].

Эта тенденция имеет решающее значение для обеспечения безопасности всех подключенных устройств.

Внедрение архитектур нулевого доверия

Внедрение архитектуры нулевого доверия влияет на методы управления уязвимостями устройств. Принципы нулевого доверия предполагают, что ни одному устройству или пользователю по умолчанию не доверяют, даже если они находятся в пределах периметра сети.

Этот подход требует постоянной проверки и аутентификации, что приводит к необходимости в динамических решениях по управлению уязвимостями, которые могут адаптироваться к строгим требованиям безопасности модели нулевого доверия.

Человеческий фактор остается решающим

Социальная инженерия – это распространенный метод, используемый red teams, службами тестирования на проникновениях и злоумышленниками для обхода мер контроля и получения первоначального доступа к системам организации [5].

Злоумышленники рассылают миллионы писем ежедневно, все что нужно для успешной атаки, – это нажать на одно или два письма.

Можно считать свой бизнес взломанным, как только пользователь нажмет на вредоносную ссылку – независимо от того, сколько денег было вложено в инструменты.

Заключение

Рынок управления уязвимостями устройств быстро развивается, что обусловлено необходимостью противодействия постоянно расширяющемуся спектру киберугроз во все более сложных ИТ-средах. Используя автоматизацию, интеграцию искусственного интеллекта и расширяя охват устройств Интернета вещей, организации могут эффективно повысить уровень своей безопасности [6].

Кроме того, акцент на искусственный интеллект и машинное обучение, внедрение архитектуры нулевого доверия еще больше стимулируют прогресс в этой области.

По мере нашего продвижения вперед эти тенденции не только будут формировать стратегии управления уязвимостями, но и по-новому определят устойчивость организаций к киберугрозам, обеспечивая более безопасную и надежную цифровую среду.

Литература

1. Pentera. Глоссарий по управлению уязвимостями [Электронный ресурс]. URL: https://pentera.io/glossary/vulnerability-management/ (дата обращения: 24.03.2024).

2. Redscan. NIST Vulnerability Analysis [Электронный ресурс]: Руководство. 2020. Version 1.0. URL: https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf (дата обращения: 24.03.2024).

3. Частикова В.А., Псеуш А.Г. Современные подходы к автоматизации управления предприятием // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2019. № 3 (246). С. 109-112.

4. Частиков А.П., Алешин А.В., Частикова В.А. Принципы создания регенеративных экспертных систем // Материалы II Международной научно-практической конференции «Информационные технологии в моделировании и управлении». Санкт-Петербургский государственный технический университет. 2000. С. 329-331.

5. Частикова В.А., Гуляй В.Г. Методика обнаружения атак социальной инженерии на основе алгоритмов анализа естественного языка // Прикаспийский журнал: управление и высокие технологии. 2022. № 3 (59). С. 61-71.

6. Схема реализации блокчейн-процессинга для обеспечения защиты b2b-портала. Хализев В.Н., Тарасов Е.С., Бачманов Д.А. Электронный сетевой политематический журнал "Научные труды КубГТУ". 2019. № 6. С. 149-155.

7. Verified Market Reports [Электронный ресурс]. URL: https://www.verifiedmarketreports.com/blog/top-7-trends-in-device-vulnerability-management-for-2024/ (дата обращения: 24.03.2024).

Черемных Валерий Юрьевич,
старший преподаватель кафедры
уголовно-правовых дисциплин и криминалистики
Донецкого филиала Волгоградской академии МВД России

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК ФАКТОР УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Постановка проблемы**.** Стремительное развитие информационных технологий, масштаб применения глобальных телекоммуникационных сетей и процесс построения информационного общества обусловили возникновение новых угроз в информационной сфере, одной из которых является использование возникающих возможностей в террористической деятельности, что наносит ущерб жизненно важным интересам лица, общества и государства. В таких условиях стремительно растет уровень угрозы информационного терроризма в информационном пространстве.

Бесспорно, что сегодня Интернет усложнил защиту информационных ресурсов. Террористические группы и отдельные террористы во всем мире пользуются его особенностями и преимуществами, пытаясь влиять как на внутреннюю, так и на внешнюю политику государств, используя разнообразные информационные технологии для достижения своей преступной цели[1].

Так, по мнению Я.С. Гродзенского - доступность информационных технологий значительно повышает риски проявления информационного терроризма, а развитость и доступность информационной инфраструктуры общества создает «благоприятную почву» дополнительных рисков информационного терроризма, который в современных условиях глобализации и интернационализации приобретает чрезвычайно деструктивное значение[2]. В свою очередь, проблематика борьбы с информационным терроризмом требует анализа различных кризисных явлений и структуры самого терроризма как явления, которое прошло долгий путь эволюции от одиночек-смертников, впоследствии - хорошо организованных и скоординированных террористических организаций, совершающих теракты, влекущие за собой гибель большого количества людей, до использования информации для устрашения значительного количества народных масс.

Таким образом, исследование феномена информационного терроризма в контексте информационной безопасности является крайне актуальным в современных реалиях функционирования российского общества именно через призму вопросов национальной безопасности.

---

[1] Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. - М.: Инфра - Инженерия. - 2024. - 156 с.

[2] Гродзенский Я. С. Информационная безопасность. Учебное пособие. - М.: РГ-Пресс. - 2024. - 144 с.

Анализ последних исследований и публикаций. Теоретические аспекты противодействия информационному терроризму исследовали А.Н. Баланов, Л.В. Галыгина, Я.С. Гродзенский и др.

Особенности информационного терроризма как одного из способов информационной войны освещены в трудах М.А. Федотова, Ю.Н. Сычева, А.В. Царегородцева и др.

Современные угрозы информационного терроризма исследовали О.Г. Швечкова, С.И. Бабаев.

В то же время, среди ученых существуют разногласия относительно форм и разновидностей информационного терроризма, а также отсутствует комплексный подход к определению места информационного терроризма в системе угроз национальной безопасности государства, что также подчеркивает актуальность рассмотрения проблематики информационного терроризма.

Целью статьи является определение особенностей информационного терроризма как фактора угрозы национальной безопасности государства.

Изложение основного материала. Несмотря на многочисленные публикации, посвященные различным аспектам феномена информационного терроризма, должного научного осмысления среди ученых и практиков данная проблема не достигла. Кроме того, отсутствует единство подходов к пониманию такого явления как «информационный терроризм», его унифицированного толкования в доктрине информационного права до сих пор не существует[1].

Так, отдельные авторы делают довольно удачные попытки исследовать вопросы правового обеспечения информационной безопасности, отстаивая в своих трудах несколько точек зрения на рассматриваемую проблему.

Первая из точек зрения сводится к тому, что информационный терроризм рассматривается как сфера негативного влияния на отдельную категорию лиц, общество в целом, государство за счет всех видов информации с целью ослабления или свержения конституционного строя, при помощи информационно-телекоммуникационных технологий.

Анализ системы информационного терроризма часто ограничен пределами исключительно интеллектуальной сферы - наиболее перспективных видов терроризма, порождающий новый вид «насилия» в киберпространстве, которое может быть направлено против любого члена общества, а «его успех обеспечивается не грубой силой, а нейронами»[2].

Иная точка зрения состоит в исследовании информационного терроризма как запугивания общества за счет применения высоких технологий для достижения политических, религиозных или идеологических целей, а

---

[1] Информационное право: учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. - 2-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2023. - 868 с.

[2] Царегородцев А. В., Дербин Е. А. Информационное противоборство. Концептуальные основы обеспечения информационной безопасности. - М.: Инфра-М. - 2024. - 267 с.

также совокупности действий, которые приводят к отключению, выводу из строя объектов критической инфраструктуры или уничтожению информации. Такие действия могут включать использование информационных технологий для организации и выполнения атак против телекоммуникационных сетей, информационных систем и коммуникационной инфраструктуры[1].

Перспективным видится направление исследования, согласно которому информационный терроризм является разновидностью террористической деятельности, которая связана с достижениями в сфере информационных технологий.

Так, О.Г. Швечкова под «информационным терроризмом» предлагает понимать новый вид террористической деятельности, ориентированный на использование различных форм и методов временного или необратимого вывода из строя информационной инфраструктуры государства или ее элементов, а также с помощью противоправного использования информационной структуры для создания условий, влекущих тяжкие последствия для различных сторон жизнедеятельности личности, общества и государства в целом[2].

В свою очередь, правоохранительные органы в пределах своей компетенции обязаны активно противостоять угрозам информационного терроризма. По мнению А.В. Щербак - главные угрозы в сфере информационного терроризма преимущественно создают иностранные государства, международные террористические и другие преступные группировки и организации, которые пользуются порой неразвитостью и слабостью соответствующих государственных структур. Поэтому не случайно бытует мнение, что современный информационный терроризм характеризуется как множество «информационных войн» и акций с национальными или транснациональными криминальными структурами и спецслужбами иностранных государств[3].

Дефиниции «информационного терроризма» на сегодняшний день не содержат международные правовые акты, среди которых стоит выделить такие как: «Конвенция Совета Европы о предотвращении терроризма» (англ. «Council of Europe Convention on the Prevention of Terrorism» (CETS No. 196)), «Конвенция о киберпреступности» (англ. – «Convention on Cybercrime» (CETS No. 185))[4].

Так, определение информационного терроризма, с учетом различных мнений ученых-правоведов, видится как доктринальное понятие теории информационной безопасности, под которым понимают:

- общественное опасное деяние, которое является проявлением терроризма;

---

[1] Чернова Е. В. Информационная безопасность человека. М.: Юрайт. - 2023. - 328 с.

[2] Швечкова О. Г., Бабаев С. И. Информационная безопасность. Часть 1. Теоретические основы. Учебник. - М.: КУРС. - 2022. - 144 с.

[3] Щербак А. В. Информационная безопасность. - М.: Юрайт. - 2023. - 260 с.

[4] Швечкова О. Г., Бабаев С. И. Информационная безопасность. Часть 2. Стандарты и документы. Учебник. - М.: КУРС. - 2022. - 144 с.

- форму деструктивного информационно-психологического воздействия на личность, общество и государство;

- общеопасные деяния, направленные на информационное воздействие на социум, органы государственной власти, связанные с распространением информации, содержащей угрозы преследованием, физической расправой искажение объективной информации, вызывающей возникновение кризисных явлений в государстве, нагнетание паники, страха, состояния напряженности в обществе;

- определенное насильственное пропагандистское воздействие на психику человека, которое не дает ему возможности критически оценивать полученную информацию;

- множество информационных войн и информационных акций, связанных с национальными или транснациональными криминальными структурами и спецслужбами иностранных государств;

- идеологически обоснованную практику воздействия, направленного на запугивание населения, на принятие решения или совершение действий (бездействия) органом власти, международной организацией, социальной группой, юридическим лицом или физическим лицом в пределах информационного пространства, связанного с использованием информации информационных технологий и (или) информационного ресурса.

Классификация преступных деяний, составляющих такое понятие, как «информационный терроризм», предложена на рисунке 1.

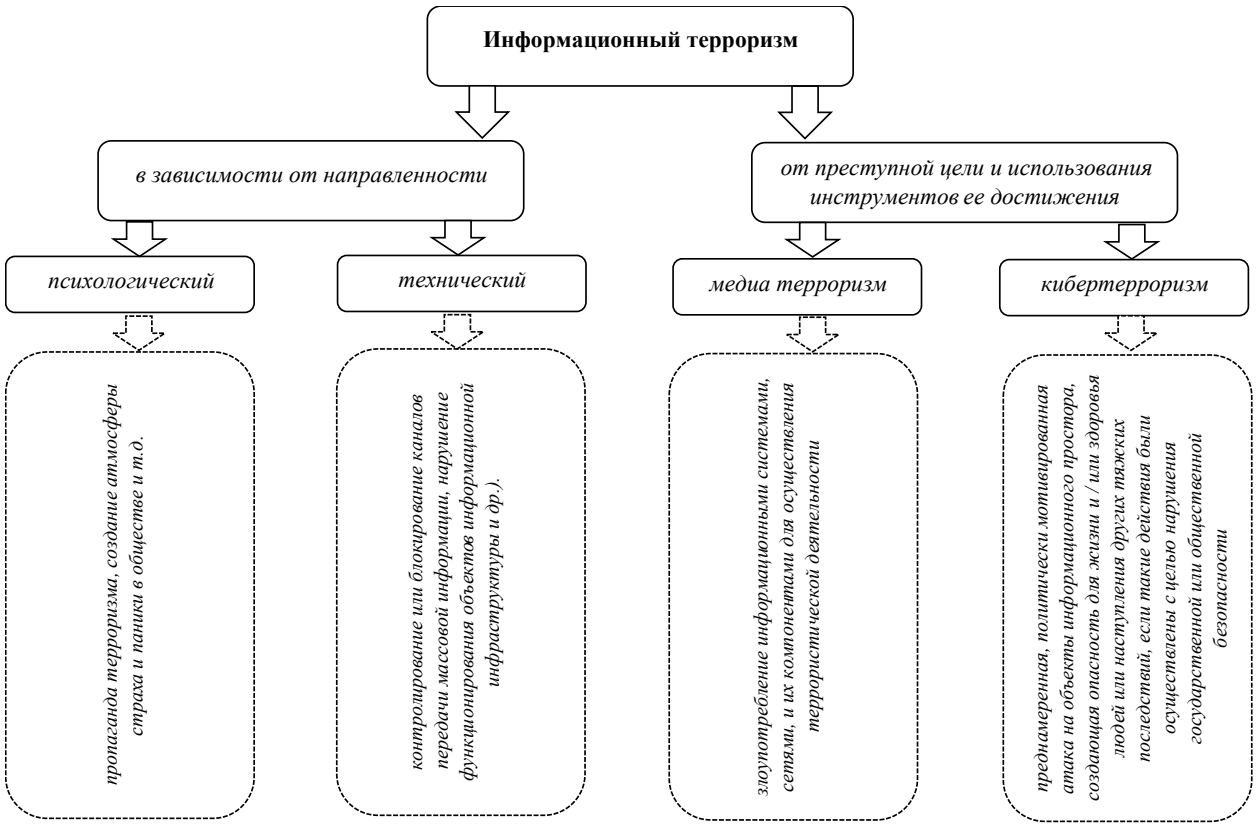


Рис. 1. Виды информационного терроризма

Так, «кибертерроризм» представляет собой в т.ч. политически-мотивированное посягательство на объекты информационного пространства, своим фактом создающее опасность для жизни (здоровья) человека (общества) или наступления других тяжких последствий, если такие действия были осуществлены с целью нарушения государственной или общественной безопасности, запугивания населения, провокации военного конфликта или угроза совершения таких действий.

Политически мотивированные атаки, наносящие серьезный ущерб, к примеру - серьезных экологических трудностей или длительных остановок энерго-, водоснабжения, можно также характеризировать как кибертерроризм[1].

В научной литературе кибертерроризм также рассматривается как террористическая деятельность, осуществляемая в киберпространстве или с его использованием. Такое преступное посягательство является крайне серьезной общественно-политической угрозой для мирового сообщества, в сравнении даже с отдельными видами оружия массового поражения - ядерным, бактериологическим, химическим оружием, виду новизны последней - не до конца осознанной и изученной. Отдельные специалисты по кибербезопасности прогнозируют, что «новые террористы» направят свои усилия на освоение информационного оружия, разрушительная сила которого может быть во много раз больше биологической и химической[2].

Кибертерроризм не имеет государственных границ; кибер преступник способен в равной степени угрожать информационным системам, расположенным практически в любой точке мира путем использования специального ПО, предназначенного для несанкционированного проникновения в компьютерные сети удаленной кибератакой.

Основной формой кибертерроризма является информационная атака на компьютерную информацию, способы и устройства передачи электронных данных, осуществляемая преступными группировками или отдельными лицами. Следствием такой атаки является проникновение в информационно-телекоммуникационную сеть или коммуникационную инфраструктуру, перехват управления, устранение средств сетевого информационного обмена и осуществление других деструктивных действий.

Для определения таких угроз следует, прежде всего, выяснить сущность понятия «угроза», которое в литературе определено как явления и факторы, которые негативно влияют или могут повлиять на определенный объект или представлять опасность нарушения интересов определенных субъектов. В свою очередь, под «угрозами национальной безопасности государства» следует понимать явления, тенденции и факторы, которые делают невозможным или затрудняют или могут сделать невозможным или усложнить

---

[1] Сычев Ю. Н. Защита информации и информационная безопасность. Учебное пособие. - М.: Инфра-М. - 2023. - 201 с.

[2] Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. - М.: Лань. - 2021. - 64 с

реализацию национальных ресурсов и сохранение национальных ценностей государства[1].

В литературе существуют разные подходы к определению угроз национальной безопасности в зависимости от объекта воздействия. В частности, одной из угроз национальной безопасности государства называют киберугрозу - объективную существующую возможность совершения киберпреступлений, вследствие чего могут наступить негативные последствия как в реальной, так и виртуальной среде для жизненно важных интересов государства.

В свою очередь, угрозы в информационной сфере следует рассматривать как факторы, наносящие вред информационной безопасности государства. Так, М.А. Федотов угрозы информационного характера рассматривает как имеющиеся или потенциально возможные явления и факторы, которые создают опасность жизненно важным интересам человека и гражданина, общества и государства в информационной сфере. Среди угроз национальной безопасности в информационной сфере автор выделяет: создание, распространение информации с целью поддержания, сопровождения или активизации террористической деятельности, проявление киберпреступности, кибертерроризма[2].

С учетом изложенного, основной задачей развития системы кибербезопасности отечественного медиапространства видится гарантирование киберустойчивости и кибербезопасности национальной информационной инфраструктуры, в частности в условиях цифровой трансформации, а среди приоритетных задач правоохранительных органов, а также специальных служб - активное и эффективное противодействие подрывной деятельности, предотвращение терроризма.

Противодействие рассматриваемой проблематике распространения киберпреступности и кибертерроризма должно включать в себя такие направления деятельности, как:

- унификация и гармонизация национального законодательства и международных актов;

- проведение научных разработок в сфере создания современных технологий обнаружения и противодействия криминальным и террористическим влияниям на информационные ресурсы;

- создание специализированных подразделений в сфере борьбы с компьютерными преступлениями и компьютерным терроризмом;

- совершенствование международного организационно – правового взаимодействия по вопросам противодействия компьютерной преступности и компьютерному терроризму; совершенствование многоуровневой системы подготовки кадров в сфере информационной безопасности.

---

[1] Щербак А. В. Информационная безопасность. - М.: Юрайт. - 2023. - 260 с.

[2] Информационное право: учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. - 2-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2023. - 868 с.

Выводы. Таким образом, одной из основных угроз информационной безопасности целесообразно определить информационный терроризм как форму деструктивного влияния, направленного на манипуляцию или запугивание населения или причинение с использованием информационных технологий вреда обществу, государству или отдельным лицам с целью принудить органы государственной власти, международную организацию, юридическое или физическое лицо (группу лиц) совершить какое - то действие (или уклониться от его совершения).

Национальная система противодействия терроризму, в том числе в сети Интернет, должна охватывать не только контрольно-надзорные и репрессивные меры.

Важно также повышать интеллектуальный уровень населения. Это поможет сформировать у граждан установки для самостоятельного отторжения террористических идеологий и практик, что будет способствовать обеспечению национальной безопасности отечественного государства.

Литература

1. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. - М.: Инфра - Инженерия. - 2024. – 156 с.

2. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. - М.: Лань. - 2021. – 64 с.

3. Гродзенский Я. С. Информационная безопасность. Учебное пособие. - М.: РГ-Пресс. - 2024. – 144 с.

4. Информационное право: учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. - 2-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2023. – 868 с.

5. Сычев Ю. Н. Защита информации и информационная безопасность. Учебное пособие. - М.: Инфра-М. - 2023. – 201 с.

6. Царегородцев А. В., Дербин Е. А. Информационное противоборство. Концептуальные основы обеспечения информационной безопасности. - М.: Инфра-М. - 2024. – 267 с.

7. Чернова Е. В. Информационная безопасность человека. М.: Юрайт. - 2023. – 328 с.

8. Швечкова О. Г., Бабаев С. И. Информационная безопасность. Часть 1. Теоретические основы. Учебник. - М.: КУРС. - 2022. – 144 с.

9. Швечкова О. Г., Бабаев С. И. Информационная безопасность. Часть 2. Стандарты и документы. Учебник. - М.: КУРС. - 2022. – 144 с.

10. Щербак А. В. Информационная безопасность. - М.: Юрайт. - 2023. – 260 с.

Шайдаев Мирзабек Шайдаевич,
старший научный сотрудник
ФКУ НПО «Специальная техника и связь» МВД России,
кандидат юридических наук

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ И ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

В рамках реализации основополагающей цели правоохранительной деятельности государства, одной из основных задач, возложенных на МВД России, является противодействие преступности, охрана общественного порядка и собственности, обеспечение общественной безопасности.

Экстремизм и терроризм представляют крайние формы преступности, отличающиеся большой общественной опасностью и тяжкими общественно-опасными последствиями, в связи с чем Министерством принимаются соответствующие меры, направленные на выявление, предупреждение и пресечение экстремистской деятельности, обеспечение участия органов внутренних дел в мероприятиях по противодействию терроризму, в том числе в обеспечении правового режима контртеррористической операции, защите потенциальных объектов террористических посягательств и мест массового пребывания граждан[1].

Основная функция по противодействию терроризму и экстремизму возложена на полицию, которая в своей деятельности использует достижения науки и техники, в том числе информационные технологии и системы, а также современную информационно-телекоммуникационную инфраструктуру[2] с целью формирования новых, отвечающих требованиям актуальности и обладающих высокой результативностью способов противодействия современным вызовам и угрозам безопасности общества и государства.

Существенной составляющей противодействия экстремистской деятельности и терроризму является выявление их проявлений в окружающей действительности с целью их предупреждения, профилактики и пресечения.

Учитывая, что основная часть экстремистских и террористических проявлений в последние годы переместилась в сферу информационно-коммуникационных технологий, как интернет и социальные сети, об эффективном выявлении указанных проявлений без использования современных информационных технологий в настоящее время говорить не приходится. Технологии искусственного интеллекта в этой связи стали признаваться одним

---

[1] Указ Президента РФ от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации». Электронный ресурс: https://base.garant.ru/71572244/?ysclid=lwa9r78 y4d145119386. (Дата обращения 13.09.2022).

[2] Федеральный закон «О полиции» от 7 февраля 2011 г. № 3-ФЗ. Электронный ресурс: https://base.garant.ru/12182530/?ysclid=lwa9t05tcu912272389. (Дата обращения 13.09.2022).

из наиболее эффективных средств, нашедших применение в правоохранительной деятельности.

Искусственный интеллект, получивший стремительное развитие и нашедший в настоящее время применение во многих сферах нашей жизни, может стать действенным инструментом в борьбе с терроризмом и экстремизмом и позволит правоохранительным органам автоматизировать ряд решаемых в этой связи задач в сфере аналитики больших объемов информации, выявления интересующей информации, прогнозирования будущих событий, мониторинга интернет-пространства.

В целом, возможности искусственного интеллекта в противодействии экстремистской деятельности и терроризму уже используются по ряду направлений.

1. Распознавание экстремистских материалов в сети Интернет.

Обученные на основе огромных массивов данных, включающих признаки материалов, отнесенных федеральным законом к экстремистским, при помощи специально разработанных алгоритмов искусственного интеллекта производится оценка информационных материалов на предмет признания их экстремистскими. Существующая система обучения современных искусственных нейронных сетей позволяет достигать контекстного понимания целых предложений или даже абзацев текста. Кроме того, создаются решения, выявляющие признаки экстремистских материалов не только в текстах, но и в изображениях, и видеоматериалах. Дополнительно возможности искусственного интеллекта реализуются в решениях как для прогнозирования последующего распространения деструктивных материалов, так и для выявления устройств, с которых производилась публикация[1].

2. Мониторинг социальных сетей.

Системы на основе искусственного интеллекта, фильтрующие контент в социальных сетях, представляют собой специальные обучаемые системы, которые распознают контент, направленный на пропаганду терроризма или экстремистской деятельности, или содержащий информацию о планировании совершения террористического акта. По статистике почти 60% преступников перед тем как совершить теракт, публикуют записи об этом в своих профилях в социальных сетях[2]. Например, устроивший стрельбу в казанской школе Ильназ Галявиев за несколько дней до этого создал Telegram-канал,

---

[1] Березина О.Б. Искусственный интеллект и противодействие экстремизму // Актуальные вопросы образования. Формирование механизмов системы высшего образования в России: сб. материалов нац. науч.-метод. конф., Новосибирск, 14–16 марта 2023 г.: в 3 ч. – Новосибирск: Изд-во СГУГиТ, 2023. – Ч. 3. – С. 212–215. Электронный ресурс: URL: https://sgugit.ru. (Дата обращения 13.09.2022).

[2] Гедгафов М.М. Роль искусственного интеллекта в противодействии терроризму // Журнал прикладных исследований. Вологда. 2023. № 8. С. 91-95. Электронный ресурс: URL: https:// cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-protivodeystvii-terrorizmu. (Дата обращения 13.09.2022).

где написал, что нападет на гимназию, после чего совершит самоубийство[1]. Искусственный интеллект, обладающий способностью быстро перерабатывать значительные объемы информации, с успехом справляется с этой задачей, способствуя предотвращении как террористических актов, так и преступлений экстремистской направленности. При этом анализу могут быть подвергнуты не только публичные записи, но и сообщения в личных чатах.

3. Блокировка деструктивного контента в интернет сетях.

В ответ на использование террористическими и экстремистскими организациями генеративного искусственного интеллекта для создания фальшивых фото- видеоизображений лиц, пропагандирующих экстремизм и терроризм, с целью манипулирования мировоззрением пользователей социальных сетей и их дезинформации, потребовалось совершенствование стратегии модерации деструктивного контента. Разработка на основе технологий искусственного интеллекта инструментария по централизованному сбору террористического и экстремистского контента позволит модераторам сетей оперативно удалять непригодный контент[2].

4. Проведение профилактических мероприятий.

Огромное значение в профилактике терроризма и экстремизма придается вопросам противодействия вербовке молодежи и школьников в экстремистские и террористические организации и их вовлечению в экстремистскую и террористическую деятельность. Отдельное внимание в этой связи уделяется лицам, склонным к совершению насилия. Исследования показывают, что признаки агрессивного поведения у них отмечаются задолго до совершения общественно опасных деяний и связаны в большей степени с желанием отомстить обидчикам, оказывавших на них в детстве психологическое или физическое воздействие. Использование искусственного интеллекта для анализа ответов школьников на специально разработанный психологический тест поможет определить лиц, нуждающихся в психологической помощи с целью профилактики их асоциального поведения[3].

В дополнение к этому проводятся исследования возможностей применения искусственного интеллекта для анализа психологического портрета на основе информации из соцсетей. Системы помогут выявлять субъектов, по-

---

[1] Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. Электронный ресурс: URL: https://trends.rbc.ru/trends/social/6169691a9a794774ed3f51d6?from=copy. (Дата обращения 13.09.2022).

[2] Экстремальное влияние: искусственный интеллект и дезинформация. Электронный ресурс: URL: https://csef.ru/news/8536/. (Дата обращения 13.09.2022).

[3] Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. Электронный ресурс: URL: https://trends.rbc.ru/trends/social/6169691a9a794774ed3f51d6?from=copy. (Дата обращения 13.09.2022).

тенциально опасных для общества, прогнозировать опасное для общества поведение людей, а также вырабатывать комплекс необходимых превентивных мер[1].

5. Распознавание лиц.

Для оперативного установления личности участников преступления на первоначальном этапе проводится сбор и анализ информации, имеющей отношение к данному событию, среди которой полезной может оказаться информация, полученная с камер видеонаблюдения. В этой связи востребованность систем распознавания лиц на основе искусственного интеллекта, устанавливаемых в камеры видеонаблюдения, для идентификации лиц, подозреваемых в терроризме, является вполне ощутимой. Таким системам под силу осуществление за считанные секунды сравнения лиц, попавших в обзор камеры видеонаблюдения, с базами данных с последующей подачей сигнала об опасности силовым ведомствам. В более совершенных системах, искусственный интеллект, обученный на основе массива признаков вооруженности человека, может распознавать наличие у него оружия. При этом для достижения максимально точного результата и эффективности требуется дообучить искусственный интеллект отграничивать оружие от других похожих на него предметов (например, дрель, удочка, метла и др.), а также работать в ограниченных внешних условиях, как, например, недостаточная освещенность или ограниченность угла обзора[2].

6. Расследование преступлений

Расследование преступлений террористической направленности сопровождается выявлением и получением большого объема информации, чаще всего требующего оперативного проведения анализа для установки всех обстоятельств дела и розыска подозреваемых в преступлении. Применение искусственного интеллекта в такой ситуации может не только ускорить процесс, но и исключить возможные ошибки следствия[3].

---

[1] Лаврухин М.В. Использование искусственного интеллекта в противодействии терроризму и оптимизация требований обеспечения транспортной безопасности к объектам дорожного хозяйства // Транспортное право и безопасность. 2022. № 4(44). С. 126-143. Электронный ресурс: URL: https://trans-safety.ru/2023/01/17/lavruhin-m-v-ispolzovanie-iskusstvennogo-intellekta-v-protivodejstvii-terrorizmu-i-optimizatsiya-trebovanij-obespecheniya-transportnoj-bezopasnosti-k-obektam-dorozhnogo-hozyajstva/. (Дата обращения 13.09.2022).

[2] Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. Электронный ресурс: URL: https://trends.rbc.ru/trends/social/6169691a9a794774ed3f51d6?from=copy. (Дата обращения 13.09.2022).

[3] Евстратова Ю.А., Шапошников А.А. Перспективы использования технологии искусственного интеллекта в оперативно-разыскном обеспечении расследования и профилактики преступлений террористической направленности // Социальная компетентность. 2023. Т. 8. № 1. С. 40-46. Электронный ресурс: URL: https://www.elibrary.ru/item.asp?edn=engejf. (Дата обращения 13.09.2022).

Использование беспилотного транспорта.

Обращаясь в рамках антитеррористической деятельности к теме использования искусственного интеллекта в беспилотном транспорте, в большей части имеется в виду беспилотные летательные аппараты (БПЛА) и, прежде всего, «дроны».

Так, технологии искусственного интеллекта нашли применение в решениях безопасности аппаратно-программного обеспечения БПЛА, обеспечивающих защиту от попыток перехвата управления ими для использования в террористических целях.

Областью внедрения технологий искусственного интеллекта становятся высокотехнологичные средства обнаружения, поражения и нейтрализации беспилотников. На основе нейронных сетей создаются системы поиска места запуска БПЛА и операторов, управляющих ими, а для **принудительной посадки беспилотников используются системы нейтрализации** БПЛА**, функционирующие на базе искусственного интеллекта. Доказали свою эффективность** для защиты крупных территорий специализированные средства глушителей каналов навигации беспилотников, в которых искусственный интеллект отвечает за автоматическое определение «свой-чужой» и идентификацию беспилотников среди всех воздушных объектов.

Искусственный интеллект и оружие.

Отдельным и вместе с тем спорным направлением является внедрение искусственного интеллекта в системы, оснащенные оружием, например, беспилотный или иной транспорт, предназначенные для уничтожения террористов без участия человека. Искусственному интеллекту в указанных системах отводится роль однозначного определения цели поражения среди мирных людей.

Есть попытки создания так называемого умного оружия, в котором от искусственного интеллекта требуется за считанные секунды проанализировать и оценить окружающую обстановку с последующим определением необходимости производства выстрела. Функция принятия правильного решения возлагается на обученный для этого искусственный интеллект. Обучение основывается на законодательстве, регулирующем правомерность применения оружия[1].

7. Искусственный интеллект в системах подготовки и принятия решений.

В рамках реализации Министерского плана по внедрению технологий искусственного интеллекта в деятельность органов внутренних дел Российской Федерации на 2023-2025 годы предусматривается создание информационного сервиса обеспечения деятельности Ситуационного центра Министерства внутренних дел Российской Федерации, отвечающий за информационно-аналитическое обеспечение решения задач управления силами и

[1] Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. Электронный ресурс: URL: https://trends.rbc.ru/trends/social/6169691a9a794774ed3f51d6?from=copy. (Дата обращения 13.09.2022).

средствами органов внутренних дел в кризисных ситуациях. Задача нейронных сетей – на основе моделирования и анализа оперативной обстановки выработка управленческого решения.

Таким образом, в ситуации, когда экстремизм и терроризм остаются актуальными угрозами обществу и государству внедрение технологий искусственного интеллекта как механизма противодействия указанным угрозам следует рассматривать одной из наиболее актуальных и эффективных мер.

Литература

1. Березина О.Б. Искусственный интеллект и противодействие экстремизму // Актуальные вопросы образования. Формирование механизмов системы высшего образования в России: сб. материалов нац. науч.-метод. конф., Новосибирск, 14–16 марта 2023 г.: в 3 ч. – Новосибирск: Изд-во СГУГиТ, 2023. – Ч. 3. – С. 212–215

2. Гедгафов М.М. Роль искусственного интеллекта в противодействии терроризму // Журнал прикладных исследований. Вологда. 2023. № 8. С. 91-95.

3. Евстратова Ю.А., Шапошников А.А. Перспективы использования технологии искусственного интеллекта в оперативно-разыскном обеспечении расследования и профилактики преступлений террористической направленности // Социальная компетентность. 2023. Т. 8. № 1. С. 40-46.

4. Лаврухин М.В. Использование искусственного интеллекта в противодействии терроризму и оптимизация требований обеспечения транспортной безопасности к объектам дорожного хозяйства // Транспортное право и безопасность. 2022. № 4(44). С. 126-143.

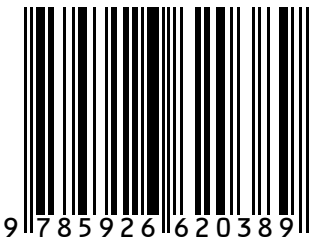
Научное издание

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции
(24 мая 2024 г.)

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2038-9



Подписано в печать 29.07.2024.
Авт. л. 7,6. Заказ 272.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.