Краснодарский университет МВД России

ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции

(18 мая 2023 г.)

Краснодар
2023

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 в противодействии экстремизму и терроризму [Электронный ресурс] : материалы Всерос. науч.-практ. конф. (18 мая 2023 г.) / редкол.: А. В. Еськов, А. С. Арутюнов, А. К. Назаров и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2023. – 1 электрон. опт. диск.

И741

ISBN 978-5-9266-1922-2

В сборнике представлены материалы Всероссийской научно-практической конференции «Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму», состоявшейся в Краснодарском университете МВД России 18 мая 2023 г.

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

УДК 316.485.6+004.7
ББК 66.4(0)+304.1

ISBN 978-5-9266-1922-2

Оглавление

Арутюнов Александр Самсонович,
кандидат юридических наук
начальник кафедры судебно-экспертной деятельности
Краснодарского университета МВД России

Еськов Николай Александрович,
эксперт отделения судебных экспертиз
экспертно-криминалистического отдела
Управления МВД России по г. Краснодару

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ ПРЕСТУПНУЮ ДЕЯТЕЛЬНОСТЬ В СЕТИ ИНТЕРНЕТ

В настоящее время интернет является неотъемлемой частью жизни людей. Каждый день появляются новейшие технологии и сервисы, улучшающие и упрощающие жизнь. Однако, помимо этих положительных сторон, интернет оказался «полем боя» преступности и правопорядка. Ежедневно и ежечасно на просторах интернета злоумышленники осуществляют преступные действия, и перед правоохранительными органами стоит задача разыскать этих преступников и привлечь к ответственности. Поэтому оперативно-розыскная деятельность с использованием интернет-технологий очень востребована.

Согласно ФЗ №149-ФЗ от 27.07.2006 года «Об информации, информационных технологиях и о защите информации», информация – это сведения (сообщения, данные) независимо от формы их представления. То есть фактически любые сведения о ком-либо или о чем-либо можно назвать информацией.

Прогрессивный мир неотступно приближается к повсеместному использованию цифровой документации. Гражданам все чаще предлагают перейти на электронные документы, будь то страховка на машину, медицинский полис и прочее, а в банках уже не один год все данные на клиентов переведены в цифровой формат и хранятся в электронном виде. Все это является весомым преимуществом для сотрудников правоохранительных органов в плане поиска информации о гражданах с помощью интернет технологий, так как они значительно ускоряют и упрощают этот процесс. Но не обходится и без негативных моментов, ведь все эти базы находятся в закрытом доступе[1], и чтобы получить из них информацию, необходимо отправлять в соответствующие организации специальные запросы, по которым ответ может быть предоставлен не так быстро, как хотелось бы. В связи с этим

---

[1] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

оперативно-розыскные мероприятия[1] в сети интернет нельзя признать достаточно продуктивными.

Если подходить к понятию интернета с точки зрения информатики, то интернет – это информационно-телекоммуникационное средство для передачи, хранения и обработки информации. В связи с тем, что интернет, по своей сути, информационно-телекоммуникационная среда, то это сказывается на специфике следов преступления, на выборе и использовании технических средств для раскрытия преступлений, на способах получения оперативно-розыскной информации и других аспектах.

С одной стороны, интернет представляет собой сервера, компьютеры, оборудование и каналы сети, но с другой стороны у него нет какой-либо привязанности к месту, отсутствуют какие-либо физические границы. Сейчас информация у вас на компьютере, а через мгновение вы можете отправить ее в любую точку мира, где есть интернет. Таким образом, интернет затрудняет работу правоохранительных органов в поиске нарушителей ввиду его виртуальной среды и не типичности по сравнению с классическим местом совершения преступления.

Теоретически, при совершении преступления в сети интернет, можно установить местонахождение преступника и потерпевшего, так как сохраняются следы преступления на устройствах потерпевшего и преступника. Однако, злоумышленник может удалить оставшуюся информацию со своего устройства или избавиться от него. Также он способен использовать несколько устройств для своего преступного умысла или выполнять какие-либо действия на одном устройстве, а продолжать их выполнение на другом. Помимо этого, возможно исполнение своих преступных действий с помощью мобильных устройств, таких как смартфон или ноутбук, и физически перемещаться в пространстве, что не позволяет конкретно определить место совершения преступления.

Кроме того, преступник может использовать специальные программы, позволяющие производить подмену данных, изменяя реальные данные на подложные. Такие программы активно используются для сокрытия определенных сайтов от обычного рядового пользователя и формируют так называемый «Дарк Нет» (теневой интернет), предназначенный, в том числе, для продажи или покупки запрещенных в гражданском обороте товаров, таких как наркотические средства, оружие, а также работорговля и прочее. Обнаружение таких сайтов и борьба с ними является особой проблемой для правоохранительных органов.

Помимо описанных ситуаций отдельную нишу занимают преступления, имеющие трансграничный характер, они приводят к наступлению об-

---

[1] Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ.

щественно опасных последствий, причем сам преступник фактически не пересекает границы государства. В таких случаях для осуществления оперативно-розыскных мероприятий необходимо международное взаимодействие, что в свою очередь вызывает определенные трудности.

Из вышеуказанного следует, что существует множество способов сокрытия преступлений, совершенных с использованием сети интернет, которые препятствуют правоохранительным органам в их раскрытии.

Специфика интернета, как киберпространства, влияет на проведение оперативно-розыскных мероприятий и по некоторым другим факторам. Один из таких факторов – это дефицит времени, что и так свойственно для оперативно-розыскной деятельности. В сети интернет этот фактор заметно усиливается в связи с недолговечностью существования информационных объектов и изменчивостью обстановки в сетевом окружении. Большинство сетевых процессов представляют из себя технологически сложные операции и имеют большой объем данных, представленных в электронном виде, что приводит к необходимости привлечения специалиста-техника для проведения оперативно-розыскных мероприятий. Специалист должен обладать необходимыми познаниями в области информационных технологий, а также техническим оснащением.

Необходимо отметить, что постоянно растет количество сайтов, предоставляющих возможность анонимного общения. Такие сайты пропагандируют свои определенные идеи, взгляды на жизнь и образ жизни, а также используются для получения информации о покупке и продаже наркотических средств, рекомендаций по их изготовлению. В последнее время бесконтактный способ передачи наркотических средств стал практически основным. На таких сайтах также осуществляется торговля оружием, поддельными денежными билетами и всевозможными похищенными данными, например, номерами кредитных карт и т.п.

Интернет становится источником опасных сведений, появляются определенные группы и целые секты по вовлечению подростков в опасную криминальную деятельность. В социальных сетях пропагандируются группы, где молодые люди, недавно вошедшие во взрослую жизнь и столкнувшиеся с трудностями, обсуждают способы совершения суицида. Более того, некоторые из них попадают под психологическое воздействие преступников, которые подталкивают их на совершение преступления или суицида. Мы помним нашумевшую в 2016 году «игру» под названием «Синий кит», когда подростки под влиянием, так называемого «куратора», выполняли определенные задания, которые заканчивались суицидом. Также к опасным знаниям можно отнести то, что на некоторых сайтах подробно описан способ изготовления взрывчатых и отравляющих веществ, а также осуществляется продажа ингредиентов для их изготовления. Такие сайты должны попадать под особый контроль сотрудников правоохранительных органов.

Следует отметить, что преступность в сети интернет создает вокруг себя новые криминальные сообщества и формирует особую криминальную

субкультуру. Оперативные сотрудники все чаще имеют дело с профессиональными преступниками, у которых высокий уровень интеллектуальной и технической подготовки. Как правило, киберпреступники хорошо осведомлены о существующих методах и средствах оперативно-розыскной работы и оказывают активное сопротивление раскрытию преступлений. Хакеры объединяются в сообщества и представляют особую криминогенную среду, которая увеличивает число латентных преступлений, что представляет особый интерес для оперативно-розыскной деятельности. Такие хакерские группировки имеют сложную организацию и сложный механизм взаимодействия участников группы. Интернет создает необходимые условия для структурной оптимизации преступных формирований. В настоящее время все реже организованная преступная группа представляет из себя крупную организацию с определенной иерархией в коллективе. Большинство хакерских групп – это временный союз для решения определенной криминальной задачи. При этом группа может включать в себя довольно большое количество лиц, которые могут находиться в разных городах и странах, что также значительно осложняет оперативно-розыскную деятельность. Совместная преступная кибердеятельность в некоторых моментах может отличаться от типичных форм соучастия. Как правило, в группе отсутствует лидер, а ее участники не знакомы лично. Координация деятельности группы осуществляется посредством общения в сети, и любой участник группы может участвовать в преступной деятельности нескольких групп одновременно.

Практика показывает, что организованные преступные группы, основанные на сетевом взаимодействии, лучше адаптируются к изменениям в привычной среде существования преступных групп и внешним воздействиям. Это обусловлено несколькими факторами. Во-первых, хакерская группа имеет гибкое управление, что обусловлено различными способами общения в сети, подбирающимися под сложившуюся ситуацию. За счет этого группа быстро реагирует на действия правоохранительных органов. Вторым фактором является отсутствие в группе локализованной структуры, т.е. один человек может выполнять разные функции, что усложняет внедрение оперативных сотрудников в группу. Третий фактор – это быстрое изменение состава группы и перераспределение ролей ее участников, что дает такой группе преимущество над группами с определенной иерархией в коллективе. При выведении из строя одного участника другой с легкостью может занять его место и выполнять его функции. А после выполнения криминальных мероприятий группа может на определенное время разойтись, что уменьшает вероятность обнаружения ее правоохранительными органами. Четвертым фактором является возможность использования различных методов для решения одной и той же задачи, что значительно затрудняет деятельность оперативно-розыскных мероприятий и не позволяет использовать стандартный подход к обнаружению таких групп. Вышеперечисленные факторы заставляют пересматривать тактику проведения оперативно-розыскных мероприятий для выявления хакерских групп в сети интернет.

Для успешного проведения оперативно-розыскных мероприятий с помощью сети интернет необходимо понимание и знание особенностей киберпреступлений. Согласно уголовному законодательству[1] к киберпреступлениям относятся общественно опасные деяния, совершенные на основе удаленного доступа к объекту посягательства с использованием сети интернет в качестве основного средства достижения цели. Список преступлений, совершаемых посредством использования интернет пространства довольно обширный. В него входят такие преступления, как мошенничество, вымогательство, хищение денежных средств с банковских счетов, незаконное получение и разглашение сведений, составляющих коммерческую тайну, нарушение авторских прав и т.д.

Преступления, совершаемые дистанционно с использованием сети интернет, можно охарактеризовать повышенной скрытностью, которая обеспечивается сложностью структуры сети и развитием способов сокрытия преступлений. Большинство киберпреступлений имеет трансграничный характер, в таких случаях как правило преступник и объект преступления попадают под законы различных государств. Способы совершения преступления являются нестандартными, сложными и отличаются своим многообразием совершения.

Киберпреступники способны делиться со своими подельниками успехами по выполнению противоправных действий, раскрывая способы совершения и результаты своей деятельности, которые могут быть использованы вновь.

Подводя итог, можно отметить, что оперативно-розыскные мероприятия в сети интернет обусловлены особенностями, связанными со свойствами сети, и требуют усовершенствования существующих способов противодействия киберпреступности. Для повышения числа раскрытий преступлений в сети интернет необходимо: во-первых, привлекать специалистов, имеющих глубокие знания в информатике и программировании, которые будут быстрее и качественнее выполнять поиск преступника. Во-вторых, разработать и внести определенные поправки в ФЗ «Об оперативно-розыскной деятельности» с целью расширения способов и методов получения подробной информации о преступлениях в сети интернет. В-третьих, повышать качество и скорость взаимодействия между оперативными подразделениями на региональном и межрегиональном уровнях. В-четвертых, создать отдельное подразделение в системе МВД, направленное на борьбу с киберпреступностью. В-пятых, оснастить оперативно-розыскные группы современным высокоскоростным интернет-оборудованием для достижения поставленных целей.

---

[1] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ

Арутюнов Александр Самсонович,
кандидат юридических наук, доцент
начальник кафедры судебно-экспертной деятельности
Краснодарского университета МВД России

Фаниев Павел Андреевич,
адъюнкт кафедры судебно-экспертной деятельности
Краснодарского университета МВД России
эксперт-организационно методического отдела
ЭКЦ ГУ МВД России по Краснодарскому краю

ОБЕСПЕЧЕНИЕ ЛИЧНОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ СБОРА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Стремительный технологический прорыв, произошедший в последние 30 лет, кардинально изменил взгляды современного человека на межличностную коммуникацию. Сегодня обмен информацией между людьми все в большей степени осуществляется не в реальном, а в цифровом пространстве. С каждым годом, все больше сервисов из реального мира находят свое отражение в виртуальной среде. Появление интернета поставило жирную точку на индустриальном этапе развития современного общества и ознаменовало начало постиндустриального этапа, характеризующегося такими аспектами как высокий уровень расширения сферы услуг. Признание информации основной производственной единицей, привело к высокому уровню развития информационных технологий. Глубокое внедрение интернета в жизнь современного человека привело к формированию одного из феноменов 21 века – цифровой личности.

Цифровая личность – это результат постоянной оцифровки персональных данных, к которым относятся индивидуальные потребности, деятельность, отношения, биография, личностные особенности и привычки.[1] Как и в реальном мире, цифровая личность имеет свои уникальные следы. К ним можно отнести, как отпечаток (fingerprint) браузера, включающий данные о ip-адресах, сведения о провайдере, cookie файлах и т.д., так и различные персональные данные, оказавшиеся в сети, как легально (в результате предоставления согласия на обработку персональных данных), так и в виду их утечки из различных баз данных.

Изучая цифровое пространство и анализируя поступающую информацию, можно получить сведения о деятельности практически любого чело-

---

[1] https://infourok.ru/cifrovaya-lichnost-rebenka-v-cifrovom-mire-3593448.html#:~:text=Цифровая%20личность%20–%20это%20такой,сети%2C%20личном%20блог%20и%20тд

века в интернете. Формированием приемов и методов подобного анализа занимается такая прикладная дисциплина как OSINT (Open Source Intelligence). Эти приемы активно используются в конкурентной разведке, но сегодня, все чаще они применяются для расследования преступлений. Вместе с тем, информационный шпионаж получил широкое распространение в криминальной среде. Так преступники, могут осуществить сбор информации об интересующих сотрудниках силовых структур и составе их семьи для оказания давления. Как правило, злоумышленника интересуют сотрудники, которые осуществляют непосредственное расследование материалов, связанных с ним напрямую. С целью обеспечения личной безопасности должностного лица, осуществляющего расследование преступления в виртуальном мире, рекомендуется соблюдать ряд правил, направленных на сохранение его цифровой анонимности.

Под цифровой анонимностью в интернете подразумеваются различные способы, направленные на сокрытие своих действий во всемирной сети[1]. В целях обеспечения анонимности возможно применение одного из трех подходов, каждый из которых имеет свои положительные и отрицательные стороны:

1) Максимальное сокрытие информации.

2) Создание фальшивой цифровой личности.

3) Комбинированный подход.

В первом случае, как следует из названия – основной задачей пользователя выступает максимальное ограничение сайтов или программных продуктов, в части сбора информации о пользователе. Это достигается путем соблюдения ряда правил:

– не использовать для работы учетные записи, содержащие какую-либо реальную информацию (например, личную почту, аккаунты в социальных сетях и мессенджерах и т.д.);

– использовать только проводное интернет соединение – оно более устойчиво к взлому;

– запретить доступ сайтам к cookie файлам пользователя – в целях минимизации риска их хищения и использования для последующей деанонимизации;

– отключить в используемом браузере JavaScript и все виды синхронизации;

– запретить использование кэш-файлы. Существует способ подмены кэша DNS-серверов для перенаправления трафика пользователя на вредоносный сайт вместо легитимного, с целью хищения информации;

– не использовать для работы незащищенное соединение по стандарту http – передаваемые данные через этот стандарт не шифруются, в силу этого передаваемые данные могут быть доступным сторонним лицам;

---

[1] https://ru.wikipedia.org/wiki/Анонимность_в_Интернете

– использовать виртуальную машину или «чистую» операционную систему;

– использовать VPN соединение (например, сеть tor), «безопасный» DNS – сервер;

– запретить использование технологии WebRTC для установления p2p-соединения. Это связано с тем, что протокол WebRTC использует серверы STUN (Session Traversal Utilities for NAT). Они хранят в себе все IP адреса которые использовались для обращения к ним, преобразуя их из домашних публичные. В результате, любой сайт, который использует эту уязвимость WebRTC в своих целях, может получить настоящий IP-адрес.

Подобный подход позволяет обеспечить довольно неплохой уровень анонимности, однако, он имеет ряд существенных недостатков. Во-первых, отсутствие возможности просмотра интернет сайтов, требующих регистрации. Во-вторых, низкая скорость обработки информации, как следствие значительное затруднение сетевого «серфинга» в поисках интересующих сведений. В-третьих, большое количество интернет сайтов не дает доступ для пользователей, о которых не может собирать информацию. Это приводит к тому, что целый ряд интернет ресурсов не используется для получения информации.

Подход, направленный на создание фальшивой цифровой личности и фальшивых отпечатков браузера, является не только более гибким для работы в сети, но и более безопасным. Также, как и предыдущем подходе, тут предусматривается ограничение передаваемой информации и использование VPN сервисов и «безопасных» DNS-серверов. Однако, масштаб устанавливаемых ограничений значительно ниже. За счет этого, достигается большая доверенность со стороны сайтов. В тоже время, за счет создания поддельной цифровой личности найти настоящие данные о пользователе гораздо труднее, не только по причине их искаженности, но и в силу того, что определенная открытость пользователя к предоставлению информации сайтам, вызывает меньше подозрений. Для реализации этого подхода так же характерно соблюдение ряда принципов:

– для работы обязательно применяется операционная система, установленная на виртуальную машину;

– подменять отпечатки браузера на наиболее популярные варианты. Например, искажая сведения об используемой версии браузера, следует провести предварительный анализ различных статистических интернет ресурсов, с целью установления наиболее популярной версии;

– подменять сведения об операционной системе и используемой аппаратуре, например, информация о видеокарте, материнской плате и т.д.;

– также необходимо изменять сведения о настройках операционной системы, например, языковые настройки, информация о расширении экрана, часовом поясе и т.д.;

– отключение технологии WebRTC;

– в случае работы в среде с искаженными сведения о цифровой личности, следует помнить, что все используемые почтовые сервисы, виртуальные платежные системы и т.д. так же должны иметь искаженные сведения.

Использование этих приемов позволяет сформировать фальшивые данные для UserAgent браузера и обеспечения дальнейшего безопасного использования интернета.

UserAgent браузера — это строка с данными, отправляемая браузером веб-сайту при подключении, в которой содержатся данные об используемой платформе (операционной системе), архитектуре, а также версии используемого браузера[1].

Комбинированный подход, в целом, аналогичен предыдущему, однако подразумевает более широкий уровень ограничений для сбора интернет сайтами видоизмененных сведений. Но такой подход применяется крайне редко.

Существует ряд способов подмены цифровых отпечатков:

1) Сокрытие информации путем замены оборудования;[2]

2) Применение антидетект браузера – специального программного обеспечения, предназначенного для подмены отпечатков браузера. Каждый из них имеет свои плюсы и минусы, однако их основной задачей в большей степени остается сохранение максимальной анонимности, и как следствие, созданием трудностей в использовании ряда интернет ресурсов. Кроме того, в виду имеющихся уязвимостей, не исключается возможность определения факта использования антидетект браузера, и как следствие дополнительные трудности в сборе информации (например, некоторые социальные сети могут удалить аккаунт, если будет выявлен факт его регистрации с использованием подобного ПО);

3) Ручная настройка браузера, созданного на базе firefox (к примеру, librewolf) – достаточно простой способ изменения своих отпечатков. Так, перейдя в настройки браузера по адресу about:config и осуществив поиск по ключевому слову resist, мы увидим все подробный перечень настроек, отвечающих не только за подмену отдельных элементов отпечатков браузера (например, настройка resist.letterboxing – отвечает за изменение информации о разрешении экрана), но и блокировку передачи ряда информации сайтам. Однако, у подобного подхода имеется ряд недостатков. Во-первых, ручная настройка требует от пользователя определенных познаний в архитектуре браузера и специфике его работы. Во-вторых, все эти настройки не несут в себе глобальной антидетект функции и направлены либо на полную блокировку передачи информации (например, cookie), либо маскировку лишь некоторых из ключевых параметров;

---

[1] https://habr.com/ru/companies/vivaldi/articles/479620/

[2] В дальнейшем рассматриваться не будет, ввиду своей затратности и нерациональности.

4) Использование расширений браузера – преимущество этого способа заключается в том, что расширения имеют более гибкий и расширенный функционал по сравнению с настройками, заложенными в браузер. Например, расширение Chameleon позволяет довольно гибко замаскировать UserAgent, искажая сведения не только о браузерных настройках, но и об используемой операционной системе.

Каждый из описанных способов имеет свои положительные и отрицательные стороны. Для достижения желаемого результата, следует рассматривать рассмотренные способы в комплексе, в зависимости от конкретно решаемой задачи. Существует ряд программных продуктов, в которых, в той или иной мере, реализованы указанные приемы обеспечения анонимности. По мнению авторов, довольно универсальным решением для обеспечения анонимности и, как следствие, личной безопасности при сборе информации в интернете, является использование браузера Venator, поскольку в нем реализовано большинство преимуществ, описанных выше. Кроме того, следует отметить, реализованную в нем функцию контейнеризации цифровой личности, которая позволяет в рамках одной рабочей сессии, использовать сразу несколько различных отпечатков бразуера, что способствует значительному повышению уровня анонимности пользователя.

Афанасьев Евгений Владимирович,
преподаватель кафедры судебно-экспертной деятельности
Краснодарского университета МВД России

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Аннотация: В статье рассматриваются риски злоупотребления алгоритмами в работе искусственного интеллекта, которые могут привести к нарушению прав человека и свободы выражения мнения, необходимость соблюдения высоких стандартов этики и правовых норм, а также обеспечения высокой точности и надежности работы алгоритмов. Раскрываются возможности искусственного интеллекта и описание того, как он может быть эффективным инструментом в борьбе с терроризмом, при условии соблюдения всех необходимых мер и правил.

Ключевые слова: экстремизм, терроризм, противодействие, искусственный интеллект.

В последние годы проблема экстремизма и терроризма стала одной из самых актуальных в мировом сообществе. В связи с этим, все большее внимание уделяется разработке новых методов и технологий, которые могут помочь в борьбе с этим явлением. Одной из таких технологий является искусственный интеллект.

Использование искусственного интеллекта в противодействии экстремизма и терроризма может быть эффективным способом выявления потенциальных угроз и предотвращения террористических актов. Интеллектуальные системы могут анализировать большие объемы информации, включая социальные сети, новостные ленты, форумы и другие источники, чтобы выявить признаки экстремистской деятельности. Также анализу могут быть подвергнуты тексты и изображения, определяться тон и настроение сообщений, выявляться ключевые слова и фразы, связанные с экстремизмом и терроризмом. Возможно использование алгоритмов машинного обучения, которые могут обучаться на основе больших объемов данных и находить скрытые связи и шаблоны в поведении пользователей.

Одним из примеров использования искусственного интеллекта в борьбе с экстремизмом является проект «Moonshot CVE». Этот проект использует алгоритмы машинного обучения для выявления экстремистских сообщений в социальных сетях. После выявления таких сообщений система предлагает контрмеры, направленные на предотвращение распространения экстремистской идеологии.

Еще одним примером использования искусственного интеллекта является система «BlueDot», которая использует анализ больших данных для выявления угроз здоровью на мировом уровне. Система может предупредить о

возможных эпидемиях, в том числе террористических актах с использованием биологического оружия.

Важно помнить о том, что искусственный интеллект не является самодостаточным и безошибочным инструментом. Его работа может быть искажена недостаточностью данных или ошибками в программном обеспечении. Поэтому необходимо использовать искусственный интеллект только в сочетании с другими методами борьбы с терроризмом, такими как разведка, оперативно-розыскная деятельность и т.д.

Также важно учитывать, что использование искусственного интеллекта может привести к нарушению прав человека на конфиденциальность и защиту персональных данных. Поэтому необходимо обеспечивать максимальную защиту данных пользователей и использовать только те данные, которые были получены легальным путем.

Кроме того, необходимо учитывать этические аспекты использования искусственного интеллекта. Например, необходимо обеспечивать прозрачность в работе алгоритмов и объяснять принципы их работы. Важно и необходимо учитывать возможные ошибки алгоритмов и предусматривать механизмы обжалования решений, принятых на основе работы искусственного интеллекта.

Особенно следует учитывать возможное использование искусственного интеллекта в целях дискриминации. Например, алгоритмы могут основываться на статистических данных, которые могут быть искажены из-за предвзятости в отношении определенных групп населения. Поэтому необходимо обеспечивать баланс между эффективностью алгоритмов и справедливостью, и равноправием для всех групп населения.

Не остается без внимания и возможность злоупотребления искусственным интеллектом. Например, некоторые государства могут использовать его в целях шпионажа или против своих политических оппонентов. Поэтому необходимо устанавливать жесткие правила и контроль за использованием искусственного интеллекта в целях борьбы с терроризмом.

Как возможный вариант развития событий следует обратить внимание и на такой аспект как риск использования искусственного интеллекта в целях угнетения населения и нарушения прав человека. Например, алгоритмы могут использоваться для мониторинга и контроля за активистами и диссидентами, что может привести к нарушению их прав на свободу выражения мнения и свободу собраний. Поэтому необходимо установить строгие правила и механизмы контроля за использованием искусственного интеллекта, чтобы избежать возможных злоупотреблений.

Кроме того, необходимо учитывать возможные ошибки и сбои в работе искусственного интеллекта, которые могут привести к неправильным решениям и негативным последствиям.

Например, алгоритмы могут ошибочно определять подозреваемых или невиновных людей, что может привести к ошибочным арестам и преследованиям. Поэтому необходимо обеспечивать высокую точность и надежность работы искусственного интеллекта.

В целом же, использование искусственного интеллекта в борьбе с терроризмом требует соблюдения высоких стандартов безопасности и урегулирования определенных правовых норм. Следует также учитывать возможные риски и злоупотребления, предусматривать механизмы контроля и обжалования решений, а также обеспечивать высокую точность и надежность работы алгоритмов. Только в таком случае искусственный интеллект может стать эффективным инструментом в борьбе с терроризмом и сохранении безопасности граждан и его использование в противодействии экстремизма и терроризма может быть эффективным способом борьбы с этими явлениями.

Литература

1. Стригуненко, Ю. В. Роль правоохранительных органов в противодействии экстремизму / Ю. В. Стригуненко // Вестник Краснодарского университета МВД России. – 2011. – № 2(12). – С. 72-79. – EDN PXZBZF.

2. Афанасьев Е.В. Актуальные вопросы оперативно-розыскного противодействия незаконному обороту специальных технических средств, предназначенных для негласного получения информации // В сборнике: «Актуальные проблемы криминалистики и судебной экспертизы». Материалы международной научно-практической конференции. Восточно-Сибирский институт Министерства внутренних дел Российской Федерации (Иркутск) 13–14 марта 2020 года. Стр. 8-10.

3. Миролюбов С.Л. Актуальные вопросы назначения криминалистических экспертиз при расследовании преступлений экстремистской и террористической направленности // С.Л. Миролюбов// журнал «Право: ретроспектива и перспектива», N 2 (6), апрель-июнь 2021 г.

Батоев Владимир Батоевич,
кандидат юридических наук, доцент,
старший научный сотрудник ФКУ НПО
«Специальная техника и связь» МВД России

ИСПОЛЬЗОВАНИЕ MESH-МЕССЕНДЖЕРОВ ПРИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ НЕСАНКЦИОНИРОВАННЫХ СОБРАНИЙ, МИТИНГОВ, ДЕМОНСТРАЦИЙ, ШЕСТВИЙ ИЛИ ПИКЕТИРОВАНИЙ В ЭКСТРЕМИСТСКИХ ЦЕЛЯХ

В современном обществе человеку ежедневно приходится сталкиваться с техническими новинками, такими как искусственный интеллект, нейронные сети, большие данные, машинное обучение и др. Безусловно, приходится констатировать факт, при котором современные информационно-телекоммуникационные технологии плотно вошли в вопросы организации жизнедеятельности человека, общества и государства в целом.

Наибольшие изменения в условиях тотальной цифровизации общества претерпевает информационно-телекоммуникационная сфера, где вопросы создания, обработки, передачи и хранения информации вышли на качественно иной уровень.

В условиях цифровой эпохи «4.0», где уже не мыслим сам факт существования человека без сети Интернет и сотовой связи, продолжают пользоваться постоянно нарастающим спросом средства мобильной связи, а также постоянно совершенствующиеся способы обмена информацией. Как и в любом социальном явлении, современные технологии передачи и обмена информацией нашли применение в криминальных целях. Не нуждается в каком-либо обосновании факты использования мессенджеров в противоправной деятельности.

Изучение практики показывает о наличии практики противодействия использованию самого современного способа передачи и обмена информацией при подготовке и совершении преступлении – так называемых мессенджеров.

Однако преступность не стоит на месте, и постоянно совершенствует свои механизмы и инструментарий.

Изучение практики показывает, что в современном обществе сформировался феномен использования технологии одноранговых сетей в криминальных целях.

В данном случае речь идет о технологии «Mesh Networks», которая иными словами представлена как самоорганизующаяся архитектуры сети. На основе данной технологии функционируют современные мессенджеры, или так называемые криптомессенджеры. Основное их отличие от обычных мессенджеров заключается в их технических особенностях функционирования. Криптомессенджеры функционируют без подключения к сети Интер-

нет, и сотовой связи, что позволяет криминально настроенным лицам использовать их в противоправных целях без какой-либо боязни быть уличенным при совершении противоправных деяний. Криптомессенджеры функционируют на основе использования технологий Wi-Fi и Bluetooth, при которых достаточно загрузить мобильное приложение и через Wi-Fi и Bluetooth обмениваться информацией.

Уже сейчас приходится констатировать акты использования мобильных приложений, функционирующих на основе технологии mesh-сетей, наиболее распространенными из которых являются «Firechat», «Bridgefy», «Signal Offline Messenger». Данные приложения активно используются при проведении несанкционированных митингов, шествий, пикетирований, протестных акциях. Ярким примером может послужить использование приложения «Firechat» при незаконных протестных акциях в 2014 году в Гонконге, что получило в дальнейшем название «революция зонтиков».

Основным «плюсом» для протестующих в тот момент выступило то, что использование данного приложения обеспечивало сквозное шифрование сообщений с невозможностью расшифровки их содержимого; отсутствие метаданных его использования на облачных хранилищах и центральных серверах, что в совокупности не позволяло идентифицировать каждого пользователя таким приложением.

К числу основных недостатков в вопросах регулирования использования подобных приложений является отсутствие подобной практики и законных оснований на использование технологии mesh-сетей в криминальных целях. Изучение юридической литературы показывает, что у правоохранительных органов имеются законные основания ограничивать права пользователей услугами связи. Однако рассматриваемые криптомессенджеры и их разработчики не являются средствами связи и их операторами соответственно.

Таким образом, можно заключить, что обозначенный правовой пробел в вопросах ограничения использования криптомессенджеров требует научного осмысления и выработки законных оснований взятия под должный контроль данного феномена. Поэтому предлагается активизироваться всем заинтересованным субъектам в вопросах мониторинга передовых зарубежных практик в целях их перенятия, а также по линии разработки правовой основы взятия использования mesh-сетей в криминальных целях.

Богданова Кристина Николаевна,
преподаватель кафедры информационной безопасности
Краснодарского университета МВД России

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ РЕАЛИЗАЦИИ УГРОЗЫ КИБЕРТЕРРОРИЗМА

Информационные технологии (ИТ) играют значимую роль в жизни общества, личности и государства. В настоящее время они используются практически во всех сферах деятельности – от банковской и медицинской до правоохранительной и военной.

Однако использование ИТ связано с рисками, связанными с утечкой конфиденциальной информации, кражей личных данных, кибератаками и другими видами киберпреступности. Киберретроризм – это одна из форм киберпреступности, основными целями которой являются подрыв социально-экономической и политической стабильности государства, ущемление прав и свобод граждан, оказание влияния на общественное мнение и привлечение внимания международного сообщества.

Поэтому обеспечение кибербезопасности означает принятие мер по защите информационных ресурсов и разработку стратегий по предотвращению кибератак и защите от угроз. Кроме того, в связи трансграничностью киберпреступлений наиболее эффективным способом борьбы с кибертерроризмом является сотрудничество государств, международных организаций и частных компаний в области кибербезопасности. Но в условиях сложной геополитической обстановки использования такого метода не представляется возможным. Представители коллективного Запада предпринимают массированную кибероперацию против нашей страны. Фактически ежедневно мощным ударам с применением продвинутых информационно-коммуникационных технологий подвергаются государственные учреждения, средства массовой информации, объекты критической инфраструктуры, системы жизнеобеспечения. Счет на вредоносные атаки против нас идет на сотни тысяч в сутки [1].

Таким образом, проблема обеспечения кибербезопасности в условиях угрозы кибертерроризма актуальна как никогда и ее обеспечению на данный момент выделена особая роль в Российской Федерации.

Для эффективного противодействия кибертерроризму необходимо выявить проблемные вопросы в деятельности должностных лиц и организаций обеспечивающих кибербезопасность. В процессе анализа законодательных и нормативно-правовых актов, регламентирующих проблематику исследования, выявленные следующие проблемы обеспечение кибербезопасности в Российской Федерации:

1. Отсутствие четкого определения термина «кибертерроризм» в законодательстве Российской Федерации. При отсутствии однозначного определения термина «кибертерроризм» затрудняется определение действий, которые можно отнести к такой форме терроризма. Также эта проблема приводит к неопределенности правового поля и, соответственно, к дезориентации правоохранительных органов при осуществлении преследования киберпреступников. Недостаточное законодательное регулирование в области кибертерроризма затрудняет создание эффективной системы противодействия кибертеррористическим угрозам.

2. Сложности в координации действий между различными ведомствами и организациями, отвечающими за кибербезопасность и борьбу с кибертерроризмом. Отсутствие единой стратегии и координации действий между ведомствами и организациями, ответственными за кибербезопасность и борьбу с кибертерроризмом, может привести к дублированию усилий и неэффективному использованию ресурсов. Недостаточность механизмов информационного обмена между ведомствами и организациями может способствовать утечкам конфиденциальной информации и затруднению работы в рамках общей стратегии.

3. Отсутствие унифицированных стандартов кибербезопасности. В данном случае организации чьи информационные системы являются объектами кибертерроризма могут использовать абсолютно разные, а зачастую недостаточные уровни защиты, а отсутствие правильно спроектированной системы кибербезопасности может породить многоуровневые уязвимости. Унифицированные стандарты кибербезопасности являются важным фактором в борьбе с кибертерроризмом и необходимы для обеспечения безопасности информации и информационных систем.

4. Неполный охват российских компаний и организаций средствами киберзащиты. В течении прошлого года все подавляющие большинство западных вендоров отказались от предоставления услуг связанных с ИТ и ИБ Российской Федерации, а собственные аналоги пока что находятся в стадии разработки, более того согласно информации, размещаемой в зарубежных средствах массовой информации, иностранными хакерскими группировками осуществляется подготовка к проведению компьютерных атак на информационную инфраструктуру РФ путем внедрения в обновления иностранного программного обеспечения вредоносных модулей, в том числе с использованием центров обновлений разработчиков иностранного программного обеспечения, размещенных в сети «Интернет [2,3]. Данная проблема усложняет реакцию на кибератаки, что может привести к дополнительным убыткам, повышенным рискам, снижению доверия к национальной кибербезопасности. В целом, отсутствие комплексного использования отечественных решений по обеспечению кибербезопасности в организациях, являющихся объектами критической информационной инфраструктуры, является угрозой национальной безопасности.

5. Низкая осведомленность пользователей о правилах безопасного использования информационных технологий. Человек является уязвимым местом в информационной системе при обеспечении кибербезопасности по нескольким причинам. Во-первых, люди могут допускать ошибки в работе с информационной системой. Например, они могут совершать ошибки при вводе данных, использовании паролей или неправильно настраивать настройки безопасности. Также кибертеррористы могут использовать техники социальной инженерии, чтобы обмануть пользователей и получить доступ к конфиденциальной информации. Охват действий их социальной инженерии может быть широким – от перехвата пользовательских данных до внедрения пользователем вредоносного программного обеспечения в информационную систему с целью дестабилизации ее работы. Часто пользователи игнорируют правила безопасности при работе с информационными системами. Например, они могут делиться информацией о своих учетных записях с другими сотрудниками. К этому приводит отсутствие осведомленности об актуальных уязвимостях и киберугрозах может привести к тому, что пользователи сами станут жертвами атак, не понимая, что происходит.

Следует избежать связывания кибертерроризма с традиционными формами терроризма. Более правильным является рассмотрение кибертерроризма как стратегии, направленной на достижение психологического эффекта. Для решения выявленных в ходе исследования проблем со стороны государства необходимо создать законодательную базу в области кибербезопасности, которая будет регулировать деятельность организаций и индивидуальных пользователей в соответствии с принципами защиты информации и борьбы с кибертерроризмом, усовершенствовоать систему обнаружения и локализации кибератак, а также методы и технологии защиты информационных систем и сетей, в том числе защиту от утечек конфиденциальной информации, создать единый и понятный алгоритм взаимодействия организаций и ведомств, которые будут заниматься выявлением и пресечением кибертеррористических актов, а также координацией действий в международном масштабе, проводить обучение и подготовку специалистов по противодействию киберпреступлениям. Вести активную работу по международному сотрудничеству с дружественными странами в области кибербезопасности. А в владельцам информационных систем необходимо гарантировать, что гарантировать, что каждое ИТ-устройство защищено и недоступно через открытые сети.

Литература

1. Antipov A. МИД России заявили, что кибероперация против России нередко напоминает терроризм [Электронный ресурс]. URL: https://www.securitylab.ru/news/530852.php (дата обращения: 15.05.2023).

2. Кибербезопасность в 2022–2023. Тренды и прогнозы // ptsecurity.com [Электронный ресурс]. URL: https://www.ptsecurity.com/ ru-ru/research/analytics/ogo-kakaya-ib/ (дата обращения: 15.05.2023).

3. Письмо ФСЭК России от 3 марта 2023 г. № 9/1925 «О мерах по повышению защищенности информационной инфраструктуры МВД России».

4. Antipov A. Кибертерроризм: виды атак, хакеров и их влияния на цели [Электронный ресурс]. URL: https://www.securitylab.ru/ analytics/537761.php (дата обращения: 15.05.2023).

5. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» | ГАРАНТ [Электронный ресурс]. URL: http://base.garant.ru/404561984/ (дата обращения: 15.05.2023).

6. Распоряжение Правительства РФ от 22.06.2022 № 1661-р «Об утверждении перечня ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России» | ГАРАНТ [Электронный ресурс]. URL: http://base.garant.ru/404891621/ (дата обращения: 15.05.2023).

7. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 – ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/ akty/53-prikazy/2270-prikaz-fstek-rossii-ot-15-yanvarya-2020-g-n-4 (дата обращения: 15.05.2023).

8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» – docs.cntd.ru [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 15.05.2023).

Гайфулин Виктор Валерьевич,
кандидат технических наук,
доцент кафедры информационной безопасности
Краснодарского университета МВД России

РОБАСТНОСТЬ КАК ИССЛЕДУЕМОЕ СВОЙСТВО АСУ СН

Характерной особенностью функционирования автоматизированных систем управления (АСУ) является существенная зависимость качества их работы от условий функционирования. Это в значительной степени определяется вариативностью параметров объекта управления в динамике реализации его целевой функции. Указанные обстоятельства в значительной степени актуальны для широкого класса автоматизированных систем, известных как автоматизированные системы управления специального назначения (АСУ СН) [1]. Это связано, в первую очередь, с тем, что нарушения в работе объектов управления этих систем приводят к существенному ущербу в той области, в которой они применяются.

С учетом того, что АСУ СН манипулируют огромными объемами информации, основным дестабилизирующим фактором в процессе их функционирования является нарушение состояний защищенности информации, и, в первую очередь состояния доступности. Блокирование доступа к информационным ресурсам АСУ СН вследствие нарушения доступности ее информации делает данную систему, как систему, функционирующую по своему целевому назначению, неработоспособной. Учитывая, что АСУ СН, по своей сути, являются системами информационными, а основным носителем угроз нарушения состояний защищенности информации в этих системах являются компьютерные атаки (кибератаки), следует рассматривать устойчивость к такого рода угрозам безопасности информации как одно из важнейших свойств, характеризующих динамику функционирования АСУ СН. С учетом этого для определения указанного свойства широко эксплуатируется термин киберустойчивость [2, 3].

Актуальность проблемы исследования киберустойчивости АСУ СН, с целью обоснования способов и средств обеспечения возможностей ее повышения, приводит к необходимости анализа ее системного характера и определения тех математических абстракций, которые с должной степенью адекватности позволяют дать количественную оценку данной характеристики как динамической.

В этой связи дадим авторскую трактовку ряда понятий, характеризующих киберустойчивость и обоснуем те математические абстракции, которые позволяют дать ее количественную оценку.

Базовым понятием, характеризующим АСУ СН, как системы, функционирующей по определенному целевому назначению, принято считать эффективность информационного обеспечения процесса управления.

Общеметодологическая трактовка понятия эффективности (лат. *effectivus*), определяет ее как степень достижения системой целей своего функционирования.

Исходя из этого, под эффективностью информационного обеспечения процесса управления будем понимать способность АСУ СН обеспечить прием, обработку и передачу информации объекту управления при использовании функционального ресурса, величина которого не превышает допустимое (требуемое) значение.

Условием, при котором считается, что АСУ СН, как информационная система, функционирует неэффективно является условие не выполнения ею своей целевой функции. В терминах приводимого выше определения это будет трактоваться как способность АСУ СН обеспечить прием, обработку и передачу информации объекту управления лишь при использовании функционального ресурса, величина которого превышает допустимое (требуемое) значение.

Что касается состояния АСУ СН обеспечить прием, обработку и передачу информации объекту управления при использовании функционального ресурса, величина которого равна допустимому (требуемому) значению, то будем считать это состояние предотказовым, а соответствующий уровень эффективности – предотказовым.

В динамике функционирования АСУ СН считается ее функционирование устойчивым, если обеспечивается уровень ее эффективности не ниже предотказового, в противном случае наступает отказ системы. Следует полагать, что соотношение отрезков времени, когда АСУ СН функционирует эффективно и когда она, вследствие кибератак, функционирует неэффективно, будет характеризовать ее киберустойчивость [4].

Учитывая изложенные ранее обстоятельства критичности АСУ СН к угрозам нарушения доступности информации будем полагать, что в качестве функционального ресурса здесь следует рассматривать временной ресурс.

Анализ системологии понятия киберустойчивости АСУ СН дает основание полагать о ее системном характере, отражающем возможности соответствующих информационных технологий этих систем - технологий обработки и защиты информации, а так же возможностей нарушителя по реализации кибератак.

С учетом временного характера функционального ресурса АСУ СН, определяющего эффективность информационного обеспечения процесса управления в этих системах, теория информационной безопасности в качестве характеристик возможностей соответствующих информационных технологий рассматривает своевременность реализации информационного процесса и своевременность реагирования на угрозы кибератак [5]. Возможности нарушителя по реализации кибератак теория информационной безопасности оценивает соответствующей вероятностью [6]

Рассмотрим математические модели, наиболее часто используемые для количественной оценки этих характеристик.

Исходя из представления условия своевременной реализации информационного процесса АСУ СН в виде:

$$\tau_{(цо)} \le \tau_{(тр)}, \quad (1)$$

характеристика $E_{(ио)}$ эффективности информационного обеспечения процесса управления в данной системе формально запишется в виде вероятности [7]:

$$E_{(ио)} = P(\tau_{(цо)} \le \tau_{(тр)}), \quad (2)$$

где $\tau_{(цо)}$ – случайная величина времени реализации цикла обработки информации в АСУ СН;

$\tau_{(тр)}$ – требуемое значение $\tau_{(цо)}$.

Представление условия (1) в виде вероятности (2) позволяет последнюю описать математической абстракцией, которая известна в классической теории вероятностей как функция распределения вероятностей [8]:

$$P\left(\tau_{(цо)} \le \tau_{(тр)}\right) \approx \int_0^{\tau_{(тр)}} f_{(цо)}(x)dx, \quad (3)$$

где $f_{(цо)}$ - функция плотности распределения вероятности случайной величины $\tau_{(цо)}$.

Основываясь на обоснованном в ряде работ [4, 5, 7] предположении о нормальном законе распределения случайной величины времени $\tau_{(цо)}$ реализации цикла обработки информации в классах систем, аналогичных АСУ СН, математическую модель характеристики эффективности информационного обеспечения процесса управления в АСУ СН можно представить в виде выражения:

$$E_{(ип)} = \mathrm{erf}\left(\frac{\tau_{(тр)} - \overline{\tau}_{(цо)}}{\sigma_{(цо)}}\right), \quad (4)$$

где $\overline{\tau}_{(цо)}$ и $\sigma_{(цо)}$ - среднее значение и среднеквадратическое отклонение случайной величины $\tau_{(цо)}$, соответственно;

erf(*) – функция ошибок.

В [4] обосновано, что среднее значение $\overline{\tau}_{(цо)}$ случайной величины времени $\tau_{(цо)}$ реализации цикла обработки информации в АСУ СН в условиях кибератак и реализации процессов защиты информации от подобного рода угроз математически представляется в виде:

$$\overline{\tau}_{(цо)} = \overline{\tau}'_{(цо)} + \overline{\tau}_{(оа)} + P_{(ка)} \cdot \left(1 - E_{(р)}\right) \cdot \overline{\tau}_{(в)}, \quad (5)$$

где $\overline{\tau}'_{(цо)}$ – математическое ожидание случайной величины потенциального (в условиях отсутствия кибератак и механизма защиты от подобного рода угроз) значения времени реализации цикла обработки информации в АСУ СН;

$\bar{\tau}_{(оа)}$ – математическое ожидание случайной величины времени обнаружения угрозы кибератаки на информационные ресурсы в АСУ СН;

$P_{(ка)}$ – вероятность угрозы кибератаки;

$E_{(р)}$ - значение характеристики своевременности реагирования на угрозу кибератаки на информационные ресурсы АСУ СН;

$\bar{\tau}_{(в)}$ - среднее значение времени восстановления процесса обработки информации в АСУ СН.

Как следует из выражения (5) динамика изменения величины времени реализации цикла обработки информации в АСУ СН, а, следовательно, и динамика изменения показателя $E_{(ио)}$ эффективности информационного обеспечения процесса управления в АСУ СН определяются динамикой угроз кибератак на информационные ресурсы данной системы.

С целью обоснования математической абстракции для разработки математической модели характеристики киберустойчивости АСУ СН воспользуемся понятием «робастность», как свойства метода, характеризующего его способность оценивать факторы, обеспечивающие независимость влияния на результат исследования различного рода выбросов [9].

Исходя из представления условия робастности функции эффективности информационного обеспечения процесса управления в АСУ СН в виде:

$$E_{(ио)} \geq E_{(отк)}, \tag{6}$$

характеристика C киберустойчивости данной системы формально запишется в виде вероятности [10]:

$$C = P(E_{(ио)} \geq E_{(отк)}), \tag{7}$$

где $E_{(отк)}$ – значение характеристики эффективности информационного обеспечения процесса управления в АСУ СН, соответствующее ее отказу, как системы, функционирующей по своему целевому назначению.

Анализируя статистическую природу представления характеристики киберустойчивости АСУ СН в виде выражения (7) представим вероятность $P(E_{(ио)} < E_{(отк)})$ события:

$$E_{(ио)} < E_{(отк)}, \tag{8}$$

противоположного событию, соответствующему условию (6) как среднее количество ситуаций, когда система, вследствие воздействия угроз кибератак на временном отрезке $[t_{(ни)}, t_{(оu)}]$ от момента $t_{(ни)}$ начала исследования до момента $t_{(оu)}$ его окончания, находилась в состоянии отказа (рис. 1):

$$P\left(E_{(ио)} < E_{(отк)}\right) = \frac{1}{I}\sum_{i=1}^{I}\alpha_i \,, \tag{9}$$

где $\alpha_i = \begin{cases} 1, \textit{при } E_{(ио)i} < E_{(отк)}; \\ 0, \textit{в противном случае}, \end{cases}$

$E_{(ио)i}$ – значение характеристики эффективности информационного обеспечения процесса управления в АСУ СН на отрезке $[t_{(н)i}, t_{(о)i}]$.

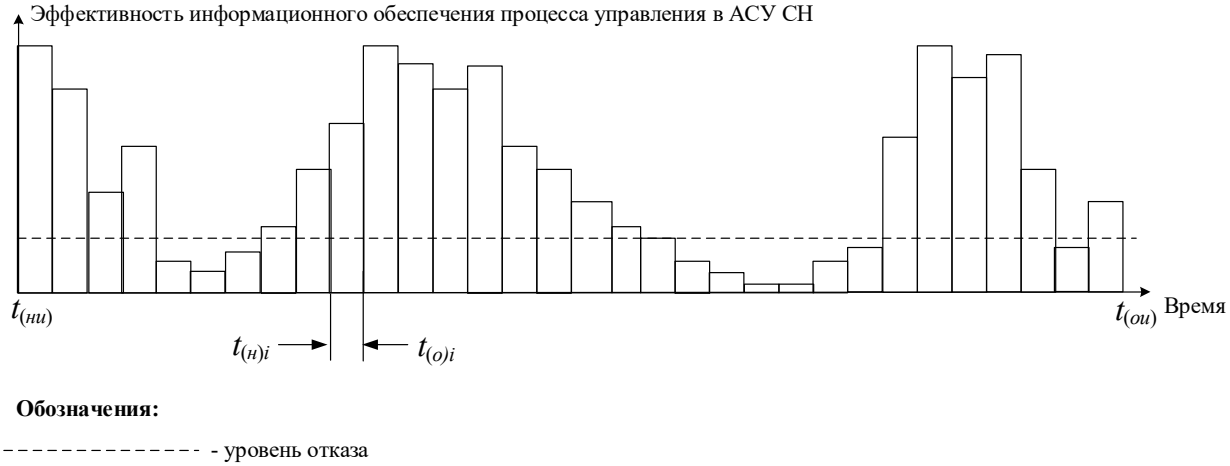


Рис. 1.

Исходя из того, что соответствующие неравенствам (6) и (8) случайные события составляют полную группу характеристика *C* киберустойчивости АСУ СН можно представить в виде выражения:

$$C = P(E_{(uo)} \geq E_{(отк)}) = 1 - P(E_{(uo)} < E_{(отк)}). \quad (10)$$

Сходство представления $P(E_{(uo)} < E_{(отк)})$ с функцией распределения вероятностей [8] позволяет описать характеристику *C* следующей математической абстракцией:

$$P\left(E_{(uo)} < E_{(отк)}\right) = \int_0^{E_{(отк)}} f_{(E)}(x)dx, \quad (11)$$

где $f_{(E)}$ - функция плотности распределения вероятности случайной величины $E_{(uo)}$.

Исходя из того, что случайный характер поведения функции эффективности $E_{(uo)}$ информационного обеспечения процесса управления в АСУ СН определяется случайным характером воздействий угроз кибератак на информационные ресурсы АСУ СН. В [4] обоснован стационарный и ординарный характер такого рода воздействий, что позволяет их описать математической абстракцией, которая известна в классической теории вероятностей как пуассоновское распределение. В этом случае период воздействия и, как следствие, ситуации, когда значения характеристики эффективности информационного обеспечения процесса управления в АСУ СН претерпевают изменения, будут иметь экспоненциальный закон распределения. Это позволяет функцию $f_{(E)}$ плотности распределения вероятности случайной величины $E_{(uo)}$ представляется в виде [10]:

$$f_{(E)}(y) = \begin{cases} 0, \textit{при } y \leq 0; \\ \dfrac{1}{\overline{E}_{(uo)}} \exp\left(\dfrac{y}{\overline{E}_{(uo)}}\right), \textit{при } y > 0, \end{cases} \quad (12)$$

где $\overline{E}_{(uo)}$ – определяется согласно выражению:

$$\overline{E}_{(uo)} = 1 - \frac{1}{I}\sum_{i=1}^{I}\alpha_i \,, \tag{13}$$

в котором вычитаемое соответствует выражению (9).

Подставив (12) в (11), а полученное выражение для $P(E_{(uo)} < E_{(otk)})$ в (10) окончательно получим:

$$C = \exp\left(-\frac{E_{(otk)}}{\overline{E}_{(uo)}}\right). \tag{14}$$

Выражение (14) является математической моделью характеристики киберустойчивости АСУ СН.

Робастный подход, как метод исследования, предполагает определение характеристики влияния выбросов на поведение функции эффективности $E_{(uo)}$ информационного обеспечения процесса управления в АСУ СН. Данная характеристика определяется в соответствии с выражением [9]:

$$S = \lim_{\Delta t \to 0} \frac{\overline{E}_{(uo)} - E_{(otk)}}{\Delta t} \,, \tag{15}$$

в котором $\Delta t = t_{(ou)} - t_{(nu)}$.

С учетом математических моделей (4), (5) и (14) характеристику (15) рассматривать как инструмент исследования киберустойчивости АСУ СН робастными методами.

Литература

1. Автоматизированные системы управления специального назначения: монография / В.Н. Козичев, А.А. Протасов, А.В. Ширманов. М.: ООО Припп «Новые авторы», 2019. 448 с.

2. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаута – СПб.: Бостонспектр, 2015. – 150 с.

3. Лукацкий А.В. Киберустойчивость, киберживучесть, кибернадежность, кибернепрерывность...http://www.iksmedia.ru/blogs/post/5445277-Kiberustojchivost-kiberzhivuchest.html#ixzz6QU4Yn2yY от 18 октября 2017.

4. Киберустойчивость информационной инфраструктуры: модели исследования: монография / В.В. Гайфулин [и др.]: под ред. С.В. Скрыля. – М.: РУСАЙНС, 2021. – 256 с.

5. Sergey Skryl, Mikhail Sychev, Artem Sychev, Tat’yana Mescheryakova, Anna Ushakova, El’vira Abacharaeva and Elena Smirnova. Assessing the response timeliness to threats as an important element of cybersecurity: theoretical foundations and research model. // Creativity in Intelligent Technologies & Data Science. (CIT&DS) 2019. Intelligent Technologies in Social Engineering. Data Science in Social Networks Analysis and Cybersecurity, Communications in Computer and Information Science 1084, Part 2. Springer Nature Switzerland AG 2019, p. 258 - 269.

6. Вероятностное представление условий своевременного реагирования на угрозы компьютерных атак / С.Е. Кондаков, Т.В. Мещерякова, С.В. Скрыль, А.Н. Стадник, А.А. Суворов // Вопросы кибербезопасности. М.: АО «НПО «Эшелон», 2019. № 6. С. 59 – 68.

7. Лаврухин Ю.Н. [и др.]. Показатели эффективности информационных процессов и их защищенности в системах реального времени. // Безопасность информационных технологий. – М.: МИФИ, 2009. – № 3. С. 104 – 106.

8. Вентцель Е.С. Теория вероятностей: Учебник (11-е изд.). - М.: КноРус, 2010. - 664 с.

9. Хампель Ф., Рончетти Э., Рауссеу П., Штаэль В. Робастность в статистике. Подход на основе функций влияния = Robust statistics: the approach based on influence functions. — М.: Мир, 1989.

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

Евлушина Дарья Николаевна,
кандидат юридических наук,
старший преподаватель кафедры предварительного расследования
учебно-научного комплекса по предварительному следствию в органах
внутренних дел Волгоградской академии МВД России

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННОЙ СФЕРЕ

Компьютерные технологии прочно и навсегда вошли в нашу современную жизнь. Двадцать первый век по праву называется информационным. В настоящее время достаточно трудно найти человека, не имеющего представления о компьютере. Стало намного проще получать необходимую информацию во всех сферах жизни. Однако и преступность с использованием высоких технологий в рассматриваемой сфере существенно выросла в последние годы во всех странах.

Глобальная сеть Интернет достигла того размаха, когда люди уже не в силах проанализировать самостоятельно все составляющие его функционирования. И чтобы повлиять на снижение деяний в информационной сфере, необходимо осуществление целого комплекса мер, направленных на достижение этой цели. Практика отмечает, что Интернет-ресурс сегодня стал одним из самых эффективных инструментов манипулирования сознанием и поведением людей.

Так же отмечается активное использование сайтов, принадлежащих террористическим и экстремистским организациям, через которые они не только обмениваются информацией, но и пытаются пропагандировать свои идеи и образ жизни, в том числе на многих языках[1].

Террористы в сети также опасны тем, что они способны атаковать или проникнуть в компьютерные системы, предприятий, организаций, банков, включая вооруженные силы, спецслужбы и т. д.

Далее рассмотрим использование современных компьютерных технологий преступными формированиями и способы противодействия им. Информационное обеспечение является основным инструментом деятельности террористических и экстремистских формирований. Оно, как правило используется в целях предания гласности своей деятельности. Современные мобильные средства связи безусловно повысили доступность преступникам в обеспечении публичности своей деятельности. Высокие технологии они используют как средство психологической войны, посредством передачи угроз, дезинформации, различных публикации на веб-сайтах наводящих

---

[1] Смирнов А.А. Информационное противодействие терроризму и экстремизму // Научный портал МВД России 2016. №4. С. 99.

ужас. Эта деятельность, несомненно, постоянно совершенствуется с увеличением объема и скорости транспортировки данных, в том числе вследствие низкой стоимости, относительного отсутствия контроля и глобальных объемов сети. Сегодня по некоторым данным насчитывается десятки веб-сайтов, созданных и поддерживаемых организациями, которые международное сообщество признало террористическими. Многие из них создаются сразу на множестве различных языков, создавая массированный источник агитации и пропаганды.

Использование преступниками онлайн-форумов, электронной почты и других средств коммуникаций «в реальном времени», несмотря на то, что аудитория многих групп невелика, их присутствие в Интернете можно ожидать, а если он имеет хороший дизайн и хорошую поддержку, это притягивает новые группы и обеспечивает им комфортное пространство[1].

Источники финансирования, способы получения и денежные потоки направлены на поддержание террористами и экстремистами своей активности. Деньги жизненно важны для них, так как являются движущей силой в их борьбе. Спектр финансирования их деятельности весьма обширен от прямых просьб о том, что организация нуждается в деньгах, благотворительных фондов, пожертвований до тайного финансирования отдельными западными государствами и США отдельных преступных формирований.

Трансформация структуры организаций также является активным способом использования мобильных средств связи и выражена в появлении новых ее форм, с учётом развивающихся коммуникаций.

Другими активными способами использования высоких технологий является сбор информации, вербовка и разведка. Преступниками используется способность сети Интернет вмещать в себя огромное количество предоставляемой пользователям информации, которую прежде чрезвычайно сложно было найти, поскольку она хранилась в разных местах и форматах.

Напротив, эффективными технологиями противодействия терроризму и экстремизму в России должны быть информационные и телекоммуникационные составляющие в виде широкого информирования общества на всех уровнях с использованием средств мобильной связи. Поскольку преступники используют в целом недостоверную информацию, в этих условиях гражданское население должно быть информировано, чтобы знать все о терроризме, экстремизме, как он проявляется в Интернете, какие сайты существуют, каковы их цели, что приводит к участию в таких группах и так далее.

Заслуживает внимание положительный опыт проведения и обсуждения актуальных проблем противодействия идеологии экстремизма и терроризма с использованием возможностей глобальной сети в формате интернет-

---

[1] Заливанский Б.В. Технологии информационного противодействия экстремизму // Современные научные исследования и инновации. 2019. №3. [Электронный ресурс] URL: https://web.snauka.ru/issues/2014/03/32751 (дата обращения 18.04.2023).

семинаров. Специалисты полагают, что следует активнее использовать возможности социальных сетей для проведения пропагандистских и контрпропагандистских акций. В данной работе необходимо максимально использовать потенциал патриотичных и популярных блогеров в Интернете, готовых к диалогу и взаимодействию в борьбе с террором. Нельзя игнорировать и тех, кто готов к сотрудничеству в формате «непрямого диалога». Также необходимо помнить, что знания равны оружию. Образованного и сознательного человека не так-то просто обмануть. В настоящее время работа по предотвращению распространения радикальных идей ведется по ряду направлений.

Диалог об экстремизме – образовательная программа предполагает ведение диалога бывших экстремистов или жертв экстремизма с потенциальной аудиторией экстремистских групп, особенно с молодежью, посредством живого общения или рассказывания их историй через видео. Общественность принимает активное участие. В программе участвуют родители завербованных боевиков.

Другое направление работы – организация взаимодействия с теми, кто ищет информацию в сети, пытаясь определиться с собственной идеологией. Для таких людей на их поиски важно создать отклик гражданского общества. Необходимо создание специального контента, объединив творческих людей и разработчиков приложений. Подобный контент распространялся бы по большинству ключевых пользователей. Крайне необходимо создать и отклик, учитывая специфику участников.

Очередным направлением является программа «Один на один», в рамках которой бывших экстремистов просят напрямую связываться с участниками групп неофашистов или экстремистов для доверительных бесед в целях изменения их позиции и взглядов. Государство в этой связи предпринимало и предпринимает различные меры по завоеванию умов членов террористических организаций, убеждая их в бессмысленности дальнейшей борьбы.

В заключении отметим, что информационные и телекоммуникационные технологии противодействия терроризму и экстремизму носят комплексный характер, они безусловно нуждаются в дальнейшем исследовании в целях выработки дополнительных эффективных мер борьбы с рассматриваемыми опасными деяниями.

Литература

1. Смирнов А.А. Информационное противодействие терроризму и экстремизму // Научный портал МВД России 2016. №4. С. 99.

2. Заливанский Б.В. Технологии информационного противодействия экстремизму // Современные научные исследования и инновации. 2019. №3. [Электронный ресурс] URL: https://web.snauka.ru/issues/2014/03/32751 (дата обращения 18.04.2023).

Евтушенко Кристина Александровна,
курсант 4 курса 1955 учебной группы
Барнаульского юридического института МВД России

Тимофеев Виктор Владимирович,
кандидат технических наук,
доцент кафедры информатики и специальной техники
Барнаульского юридического института МВД России

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: Предметом исследования является изучение практики применения технологий искусственного интеллекта в правоохранительной деятельности российской полиции. Объектом исследования в работе являются теоретические аспекты технологий искусственного интеллекта, их достоинства и недостатки, а также алгоритм работы данных технологий. В работе обсуждается практический опыт использования уже внедренных технологий, а также то как искусственный интеллект взаимодействует с правоохранительными органами. Также, рассматриваются направления в которых реализуются технологии искусственного интеллекта и актуальные проблемы применения искусственного интеллекта в настоящее время. Новизна исследования заключается в обсуждении положительных и отрицательных аспектов применения таких технологий, а также практикой использования технологий искусственного интеллекта в Российской Федерации, а также в ряде других иностранных государств. Автором приведены примеры аналитических и прогнозных моделей, а также системы «идеального общества».

Ключевые слова: искусственный интеллект, технологии искусственного интеллекта, машинное обучение, информационные технологии, алгоритм работы, направления, достоинства и недостатки, аналитические модели, прогнозные модели.

Деятельность органов внутренних дел требует постоянного развития, это обуславливается совершенствованием способов и методов совершения противоправных деяний криминальным элементом. В связи с этим, актуально рассмотреть вопросы применения технологий искусственного интеллекта (далее – ТИИ) в деятельности органов внутренних дел Российской Федерации. Это обусловлено существующим отставанием по вопросам применения ТИИ, которые требуют развития научных исследований в этой области, а также появления новых передовых достижений цифрового, технологического и научно-технического прогресса в рассматриваемой области. Немаловажно, обратить внимание на подготовку квалифицированных кадров, которые бы в будущем могли бы образовать отдельное подразделение, которое бы осуществляло борьбу с преступностью при помощи ТИИ.

Важно отметить недостатки ТИИ, к ним относят:

– стоимость внедрения, прибавив к этому затраты на установку, обслуживание и ремонт, в конечном итоге такое новшество является дорогостоящим.

– необходимость внушительного количества данных для достоверных решений, получаемых ТИИ.

– отсутствие гарантии от взлома систем и кражи данных, в результате хакерских атак.

– устранение рабочих мест, причиной для этого является автоматизирование всё большего количества задач.

Для наиболее подробного раскрытия рассматриваемой темы, важно упомянуть понятие системы искусственного интеллекта (далее – СИИ), так под ней понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать результаты, сопоставимые, с результатами его интеллектуальной деятельности. Исполнительная подсистема; база знаний и интеллектуальный интерфейс являются составляющими функциональной структуры СИИ.

Также, важно отметить алгоритм работы простейшего искусственного интеллекта (далее – ИИ), так нейросеть является одним из методов обучения ИИ. Механизм работы состоит из следующих компонентов: данные из нейронного слоя извлекаются и после обработки передают сигналы следующему слою нейронов Каждому из сигналов первоначально присваивается весовой коэффициент. Нейроны второго слоя выполняют математическое преобразование полученных сигналов и передают вычисление результатов нейронам выходного слоя. Результат выходного слоя рассчитывается исходя из данных образца. В случае его несоответствия производится доработка весовых коэффициентов. Процесс повторяется на значительном объеме данных до тех пор, пока выходное значение, сгенерированное нейронной сетью, не будет идентично образцу.

В настоящее время применение искусственного интеллекта является одним из ключевых показателей развитости страны, а также устойчивого обеспечения общественного порядка и безопасности.

Современные камеры, оснащенные ИИ, распознают нарушителей дорожного движения, так камеры способы выявлять правонарушения предусмотренные: ст. 12.6 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ)[1] «Нарушение правил применения ремней безопасности или мотошлемов», ст. 12.9 КоАП РФ «Превышение установленной скорости движения», ст. 12.36.1 КоАП РФ «Нарушение правил пользования телефоном водителем транспортного средства», а также иные правонарушения.

---

[1] Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: федеральный закон от 30.12.2001 № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Помимо административных правонарушений, ИИ помогает раскрывать различные преступления, так, например, система «Паутина» от Государственной инспекции безопасности дорожного движения (далее – ГИБДД), позволяет инспекторам ГИБДД получать данные по запросу, таким образом сотрудники могут отслеживать конкретные номера, а камеры сообщат об автомобилях с такими номерами при их фиксации. Данный комплекс окажет серьезное содействие при раскрытии преступления, предусмотренного ст. 166 Уголовного Кодекса Российской Федерации (далее – УК РФ)[1] «Неправомерное завладение автомобилем или иным транспортным средством без цели хищения». Также предусматривается выявление «автомобилей-двойников», например, при подмене идентификационного номера своего автомобиля, на номер зарегистрированный на другой автомобиль, ответственность за такое преступление предусмотрена ст. 326 УК РФ «Подделка или уничтожение идентификационного номера транспортного средства».

Таким образом, можно говорить о безусловной пользе внедрения ИИ в правоохранительную деятельность, которая к тому же подтверждена практикой.

Многие страны рассматривают применение ТИИ как одно из основных направлений развития, а также упоминают данную технологию в концепциях развития своих государств. Ведомственная программа цифровой трансформации МВД России на 2022 – 2024 годы, ставит одной из своих задач ликвидацию отставаний по вопросам применения ТИИ, это показывает, что Министерство заинтересовано в развитии данной отрасли и её активному использованию в деятельности органов внутренних дел. Для того чтобы использовать ТИИ, необходимо максимально нивелировать риски применения такой технологии, в этом направлении, в настоящее время, проводится серьезная работа[2].

Помимо вышеупомянутой программы, ТИИ упоминаются также в Национальной стратегии развития искусственного интеллекта на период до 2030 года. Так, в ней дается определение основным терминам, связанным с рассматриваемой технологией. Среди приоритетных направлений развития использования ТИИ выделяют: использование в отраслях экономики, для со-

---

[1] Уголовный Кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 13.06.1996 № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022 - 2024 годы [Электронный ресурс]: Распоряжение МВД России от 11.01.2022 № 1/37. Доступ из справ.-правовой системы «КонсультантПлюс».

здания условий для улучшения эффективности и формирования принципиально новых направлений деятельности хозяйствующих субъектов и в социальной сфере, для улучшения уровня жизни населения[1].

Важно отметить направления в которых реализуется ТИИ, к ним относят: компьютерное зрение (распознавание образцов), которое позволяет произвести биометрическую идентификацию по фото-, видео-, а также цифровому портрету, обработку естественного языка, распознавание и синтез речи, интеллектуальные системы поддержки принятия решений, перспективные методы ИИ.

В рамках реализации ТИИ, предлагается их применение для охраны общественного порядка и обеспечения общественной безопасности, в том числе для профилактики, предупреждения преступлений и административных правонарушений, а также выявления, пресечения, раскрытия и расследования преступлений и предоставления государственных услуг.

К дополнительным направлениям, в которых можно использовать ТИИ, относят линии развития ресурсного и иное обеспечения органов внутренних дел. Среди них отмечают, информационные и телекоммуникационные технологии, средства связи, системы защиты информации и кибербезопасность, а также системы и технологии ситуационного управления, научное, правовое и кадровое обеспечение, финансовое, материально-техническое и медицинское обеспечение.

Мы считаем, что развитие вышерассмотренных направлений, повысит эффективность служебной деятельности сотрудников полиции, а также прогнозируем рост производительности труда личного состава и значительное улучшение качества решения особо важных служебных задач, в следствии развития ТИИ технологий в системе органов внутренних дел.

Данные направления позволяют определить в каких структурных подразделениях органов внутренних дел использование ТИИ будет наиболее эффективно. Так, наиболее перспективным, по нашему мнению, является подразделение уголовного розыска и экспертно-криминалистическая деятельность. Например, оперативные сотрудники при проведении оперативно-розыскных мероприятий с использованием ТИИ смогут добывать наибольшее количество информации необходимой для раскрытия преступления, а при проведении различных экспертиз значительно сократить срок их проведения и получать наиболее полные результаты исследования.

Наиболее востребованными ТИИ являются:

– автоматизация рутинных производственных операций;

---

[1] О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) [Электронный ресурс]: Указ Президента РФ от 10.10.2019 №490. Доступ из справ.-правовой системы «КонсультантПлюс».

– оптимизация процессов по подбору и обучению новых кадров в системе органов внутренних дел;

– составление оптимального графика работы действующих сотрудников с учетом различных факторов и ситуаций.

Несмотря на все положительные стороны у ТИИ имеются проблемные вопросы, которые обуславливают отставание Российской Федерации в применении ИИ в органах внутренних дел.

Так, существуют проблемы в области нормативного-правового и методического обеспечения применения СИИ и ТИИ. Отсутствуют отечественные стандарты и подходы, регулирующие ТИИ и робототехнику. Это обуславливается рядом проблем, которые не имеют однозначного решения. К ним относят:

– отсутствие правосубъектности ИИ и соответствующего статуса решений, которые принимаются на основе ТИИ.

– надежность решений, которые получает СИИ и невозможность их обоснований в некоторых случаях.

– необходимость обучения СИИ, для которого требуются квалифицированные специалисты.

По нашему мнению, законодателю следует разработать национальные стандарты в области ИИ, это обеспечит снижение затрат на приложения в которых используется ИИ, а также существенно повысит эффективность оперативно-служебной деятельности действующих сотрудников органов внутренних дел, а также упразднит большую часть рутинных операций в их работе.

Также следует разработать и принять:

– нормативный правовой акт, который бы регламентировал использование ТИИ субъектами их применения в подразделениях МВД России.

– административные регламенты, которые бы допускали использование решений ИИ для принятия процессуальных решений.

– национальные (ведомственные) стандарты, в которых бы подробно разъяснись термины, связанные с СИИ, а также требования по обеспечению безопасности использования СИИ.

– учебные программы подготовки специалистов в области ТИИ, это обусловлено несоответствием числа сотрудников, желающих и умеющих развивать данное направление.

Немаловажно при рассмотрении данной темы обратиться к зарубежному опыту использования ТИИ в раскрытии преступлений. В настоящее время лидерами в исследовании ИИ являются Соединенные Штаты Америки (далее – США) и Китай. Считаем важным обратить внимание на опыт развития данных стран в рассматриваемом нами направлении.

Так, в США серьезно развито направление сбора, хранения и обработки информации, в котором ИИ и его элементы активно применяются. Информация с камер видеонаблюдения, патрульных машин, звонков, которые поступают в полицию и другие источники информации являются основой

для базы, которая потом структурируется и распределяется в единое хранилище. Создание такой системы позволило снизить преступность. Помимо вышеперечисленного, был создан сервис поиска оперативно-значимой информации из источников информации, которые до его создания не структурировались. Создание данной системы повысило эффективность работы полиции по всей стране.

Также в США развиваются аналитические и прогнозные модели. В стране разработана программа сокращения преступности с использованием статистических данных. На основе анализа данных статистики о криминальной ситуации в прогнозируемой зоне, в районе которой возможно совершение преступления и указанием предположительного времени и места их совершения, в результате такой деятельности, анализ позволил снизить уровень преступности в этих зонах.

Развито программное обеспечение, которое собирает различную информацию, в число которых входит Дезоксирибонуклеиновая кислота (ДНК), записи видеокамер и телефонных соединений, отслеживает передвижение машин, находящихся в розыске по номерным знакам и многое другое. Данное программное обеспечение позволило раскрыть и предотвратить множество преступлений в стране. Как отмечают специалисты данной компании, при помощи их разработок, удалось предотвратить не один террористический акт.

Активно развивает направление СИИ Китайская Народная Республика (далее – КНР), так помимо огромных финансовых вложений в данную отрасль, китайские пользователи генерируют существенные объемы данных, которые используют правоохранительные органы в своей деятельности.

Наиболее интересной и перспективной для рассмотрения является система «Police Cloud», которая была разработана в 2015 году Министерством общественной безопасности КНР. Данная система содержит в себе данные собираемые полицией Китая, к ним относятся: адреса проживания граждан, семейные отношения, методы контроля над рождаемостью, религиозные связи и многое другое. Система представляет собой облачные хранилища, в которой содержится полицейская информация на уровне провинций КНР.

Также, развито направление аналитических и прогнозных моделей, разработана система распознавания лиц, которая помимо информации по биометрии отслеживает действия лица, исходя и того, когда и куда ходил и что делал, на основании данной информации система прогнозирует вероятность совершения преступления. К примеру, при покупке кухонного ножа, лицо не становится подозрительным, но если к нему он докупает молоток и мешок, то рейтинг подозрительности данного лица поднимается, и данная информация поступает правоохранительным органам.

Важно отметить, систему «социального кредита» в КНР, которая с 1 января 2021 года была официально принята и юридически закреплена. Так, суть системы заключается в том, что у каждого гражданина имеется личный

социальный рейтинг, который в зависимости от поступков, совершаемых лицом может расти или опускаться. В зависимости от количества баллов данного рейтинга, определяется доступность различных сервисов в стране. Данная система настроена на создание «идеального общества», в ходе построения которого воспитывается законопослушность и человеколюбие во всех отношениях людей.

Таким образом, можно говорить об активном развитии ТИИ за рубежом, по нашему мнению, законодателю следует помимо развития собственных наработок в области СИИ, обращать внимание на опыт других государств и лучшие наработки, с адаптацией под наше законодательство и менталитет, внедрять в нашей стране.

Подводя итог, можно говорить о том, что ТИИ активно развиваются и внедряются не только в сферы общественной жизни, но и правоохранительную деятельность органов внутренних дел. Несмотря на имеющиеся отставания в данной отрасли Министерство активно внедряет новейшие технологии, а также применяет их в своей деятельности. По нашему мнению, законодателю стоит обратить внимание на разработку нормативных правовых актов, регламентов и национальных (ведомственных) стандартов, которые будут регулировать рассматриваемую сферу. Также важной задачей является разработка программ подготовки специалистов в СИИ, которые бы обучались целенаправленно для осуществления задач органов внутренних дел.

Литература

1. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: федеральный закон от 30.12.2001 № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный Кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 13.06.1996 № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022 – 2024 годы [Электронный ресурс]: Распоряжение МВД России от 11.01.2022 № 1/37. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) [Электронный ресурс]: Указ Президента РФ от 10.10.2019 №490. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Надвоцкая В.В., Рубцов И. Н., Тимофеев В.В. Разработка алгоритмов управления интеллектуальной системой инженерного обеспечения // Ползуновский альманах. – Барнаул: Изд-во АлтГТУ, 2019. – №4. – С. 94-97.

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

Еськов Николай Александрович,
эксперт отделения судебных экспертиз
экспертно-криминалистического отдела
Управления МВД России по г. Краснодару

ОБ ИСПОЛЬЗОВАНИИ ВИРУСОВ «ТРОЯНСКИЙ КОНЬ» ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК

С каждым годом информационные технологии становятся все более популярными; и без них не обходится ни одна организация. Но, тем не менее, с развитием прогресса остро стоит проблема информационной безопасности. Разработчики по–прежнему пренебрегают всевозможными методами, а также средствами защиты информации. Такое пренебрежение способно привести к негативным последствиям и скомпрометировать систему: пользователь может лишиться своих учетных записей, причём даже в нескольких приложениях, поскольку часто используется один и тот же адрес электронной почты, а иногда и один и тот же пароль. Для создателей приложений и кража данных злоумышленниками может привести к потере своей репутации и репутации продукта, следовательно, к потере клиентов, что приведёт к финансовым убыткам и расходам.

Параллельно с вредоносным программным обеспечением развивались средства антивирусной защиты. При этом с самого начала наблюдается «гонка вооружений» между вирусами и антивирусами. Первые антивирусы, как и первые вирусы, были достаточно примитивными. Антивирусы ранее представляли собой определенный набор сигнатур, на основании которых программа детектировалась как вредоносная. При этом первоначальные виды вирусов также редко видоизменялись. В связи с этим, на начальном этапе «гонки вооружений» сигнатурный анализ имел значительно больший эффект, нежели в настоящее время. В настоящий момент вредоносное программное обеспечение изменяется под каждую конкретную атаку с целью недопущения определения программы как вредоносной сигнатурным методом. Злоумышленники, как и обычные пользователи, имеют возможность бесплатно проверить сигнатурным методом любой файл на наличие вредоносного кода более чем 50–ю антивирусами. Одной из таких онлайн–платформ является Virustotal. В связи с этим, с одной стороны время жизни вредоносного кода на настоящий момент очень короткое, а с другой стороны, злоумышленники, пересобрав вредоносное программное обеспечение, имеют возможность выявить, определяется ли вирус сигнатурным методом.

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

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

Рассмотрим наиболее популярные трояны, используемые злоумышленниками для дальнейшей загрузки криптолокера.

Emotet. Данный троян уже давно используется киберпреступниками в качестве первичной компрометации. В частности, троян Emotet доставляет другой троян Trickbot, который, в свою очередь, доставляет на компьютер жертвы криптолокер Ruyk. В 2020 году в компьютерных атаках, злоумышленники (разработчики криптолокеров Prolock, Egregor, DoppelPaymer) использовали троян Emotet в сочетании с другим трояном Qakbot для получения первоначального доступа к компьютеру жертвы. Emotet, как правило, доставляется на компьютер жертвы через фишинговые письма, содержащие в себе вложенный документ Microsoft Word с вредоносными макросами.

Несмотря на то, что вредоносное вложение было открыто в программе Microsoft Word, отключенные макросы не позволили «отработать» трояну. При этом в документе Microsoft Word злоумышленники сообщили пользователю, что он должен нажать кнопку Enable Content, чтобы посмотреть содержимое письма. Неосторожный пользователь может допустить ошибку и разрешить запуск макросов. Если пользователь нажимает Enable Content, полезная нагрузка троянов Emotet или Trickbot загружалась из сети Интернет на компьютер жертвы. Следует отметить, что в самом сообщении отсутствуют трояны, так как в противном случае почтовый антивирус мог удалить сообщение.

До последнего времени Trickbot часто использовался для доставки программы-вымогателя Ryuk. Однако с недавнего времени отмечено, что операторы переключились на использование шифровальщика Conti.

В свою очередь троян Qakbot, помимо Emotet, распространяется также с использованием вредоносных скриптов Visual Basic, а также файлов Excel, содержащих макросы.

Для распространения трояна Dridex злоумышленники, вместо вложений, использовали фишинговые ссылки, по которым расположены вредоносные скрипты Visual Basic, документы Microsoft Word и Excel.

Согласно вышеизложенной информации, указанные трояны используют документы Microsoft Office, содержащие макросы. К подобным троянам также относятся IcedID (вредоносные документы распространяются в защищенном паролем архиве), Zloader (защищенные паролем электронные таблицы и документы, заархивированные скрипты Visual Basic), SDDBot (HTML-вложения для перенаправления пользователей на скомпрометированные web-сайты).

Тем не менее, не все киберпреступники использовали фишинговые атаки. Известная атака Badusb заключалась в том, что злоумышленники присылали письма по обычной, бумажной почте от имени компании BestBuy. В письме находился поддельный подарочный сертификат на 50 долларов и зараженный USB флэш–накопитель. В письме сообщалось, что на флешке находится список товаров, которые можно оплатить с помощью сертификата. После того, как usb–устройство подключено к компьютеру, выполняется powershell–команда, загружающая и запускающая бэкдор Griffon.

Многие злоумышленники, использовавшие для первоначальной компрометации письма с вредоносными вложениями, также использовали такие инструменты как PowerShell, Wimdows Command Shell, VisualBasic и даже Javascript. Например, разработчики Dridex использовали PowerShell для первоначальной загрузки с заранее скомпрометированного web-сайта. Скрипт создавал в папке %Temp% файл вида 1070400.cvr. На сетевом уровне (имеется ввиду работа в сети, а не уровень модели OSI) наблюдалась активность транспортных протоколов TCP и UDP. Через TCP–протокол осуществлялись HTTP GET–запросы к ресурсам. Часть символов в URL–адресе, из соображений безопасности, замаскирована символом #. Через UDP протокол работал протокол DNS, запрашивающий ip-адреса скомпрометированных web-сайтов в сети Интернет.

Также злоумышленники используют интерпретатор PowerShell для сетевой разведки, дальнейшей атаки и отправки данных на подконтрольные киберпреступникам сервера в сети Интернет. Помимо этого, некоторые криптолокеры распространяются в виде powershell–скрипта. Также, с помошью данного интерпретатора, удаляются теневые копии в OS Windows, чтобы у жертвы не было возможности восстановить зашифрованные данные.

В некоторых случаях системные службы, аналогично запланированным задачам, использовались для закрепления в системе жертвы. Они широко применялись для удаленного запуска полезной нагрузки и развертывания программ–вымогателей.

Кроме того, участники некоторых партнерских программ, например Egregor, использовали PsExec для продвижения по сети и выполнения полезной нагрузки Beacon путем запуска различных скриптов на удаленных хостах.

Как уже упоминалось выше, злоумышленники часто получали первоначальный доступ к целевой сети с помощью вредоносных вложений или ссылок, а также устройств BadUSB. Это значит, что для запуска цепочки заражения жертве было достаточно перейти по ссылке, открыть файл или вставить USB–устройство в компьютер. Но у этой техники есть и другая сторона. Получение доступа к привилегированным учетным записям на начальных этапах атаки давало злоумышленникам возможность запускать вредоносные программы и использовать многочисленные инструменты двойного назначения, такие как сканеры портов, вручную. Аналогичным способом они могли и разворачивать программы–вымогатели. Например, участники партнерской программы шифровальщика Dharma распространяли и запускали вымогатель вручную, используя первоначально скомпрометированный сервер для подключения к другим хостам по протоколу удаленного рабочего стола.

Кроме PowerShell, злоумышленниками часто используется технология Windows Management Instrumentation (WMI) как для локального, так и для удаленного выполнения программ. Например, операторы Emotet использовали WmiPrvSE.exe для загрузки первоначальной полезной нагрузки со скомпрометированного веб–сайта с помощью PowerShell.

Таким образом, успех реализации атаки злоумышленником даже через троянские программы часто определяется уровнем компетенций оператора, поэтому важным является своевременное повышение квалификации и обеспечение должного уровня достижения его цифровых компетенций.

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

Кальницкая Валерия Михайловна,
слушатель Краснодарского университета МВД России

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ АНАЛИЗА, МОДЕЛИРОВАНИЯ И ВОЗМОЖНОСТИ ИХ ИСПОЛЬЗОВАНИЯ ДЛЯ ВЫЯВЛЕНИЯ И ПРЕСЕЧЕНИЯ АКТОВ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

Информационные технологии в противодействии терроризму и экстремизму представляют собой совокупность методов и средств, основным предназначением которых является сбор, анализ и обработка информации в режиме реального времени, что способствует органам безопасности выявлять потенциальных террористов, предупреждать и пресекать террористические акты.

Информационные технологии противодействия терроризма и экстремизма условно можно разделить на:

1. системы массовой информации – совокупность общественных сетей (социальные сети, интернет-сообщества, блоги, форумы и т.п.), которые являются наиболее уязвимым местом в распространении террористических и экстремистских взглядов ввиду наличия высокой социальной активности, поэтому данное направление деятельности органов безопасности является в настоящее время актуальным и требующим информационных разработок;

2. системы раннего предупреждения – инструментарий, предназначенный для обнаружения и контроля опасных ситуаций, путем изучения различных аналитических компонентов таких, как социальные сети, сайты, сообщения в чатах, записи телефонных звонков, новостные каналы и др. Рассматриваемая система позволяет выявлять на ранних этапах признаки проявления терроризма и экстремизма и пресекать их;

3. системы видеонаблюдения – совокупность видеоаппартатуры и серверного оборудования, предназначенного для обнаружения, записи и хранения информации, представленной в различных видеоформатах. В настоящее время происходит активное внедрение искусственного интеллекта в системы видеонаблюдения, который позволяет путем регулярного обучения, выявлять подозрительные лица. Впервые видеонаблюдение с машинным обучением было использовано при проведении Чемпионата Мира по футболу, проводимого в г. Сочи в 2018 году, что позволило выявить скрывающихся преступников в толпе футбольных болельщиков. Однако, несмотря на хорошие результаты, система видеонаблюдения с применением искусственного интеллекта имеет явный недостаток: если преступник скроет свое

лицо (более чем на 50%) маской, солнцезащитными очками, шарфом, шапкой и т.п., то выявить его в толпе не представится возможным.

Информационные технологии в целом являются эффективным инструментом в противодействии терроризму и экстремизму, поскольку позволяет оперативно реагировать специализированным органам и организациям на угрозы личности, обществу и государству, что минимизирует число активных террористических проявлений и ущерб от возможного совершения противоправных актов такого характера.

Если рассматривать науку через призму социальной действительности, то можно сделать вывод о необходимости применения прикладных и теоретических инструментариев для моделирования и прогнозирования социально-политических конфликтов, которые в своей совокупности образовывают актуальное на сегодняшний день направление – борьбу с терроризмом и экстремизмом, что в первостепенную очередь образует наиболее простой и легитимный путь разрешения конфликтной напряженности – предупреждение насильственных угроз с использованием результатов современных информационных технологий.

В настоящее время существует небольшое количество программных решений, предполагающих анализ социальной напряженности, связанной с проявлением террористических и экстремистских взглядов (Рис. 1).

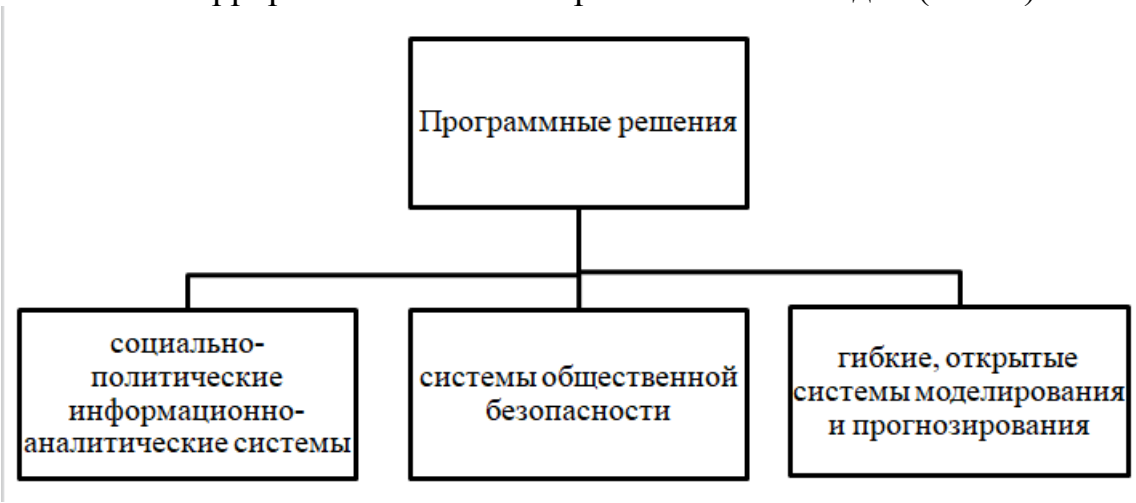


Рис.1. Программные решения для борьбы с терроризмом и экстремизмом

Рассмотрим из Рис.1 каждую подгруппу:

1) Социально-политические информационно-аналитические системы (CASCON, АРИАДНА+, «Мониторинг социальной напряженности»);

2) Системы общественной безопасности («Семантический архив», комплекс «Тренд»);

3) Гибкие, открытые системы моделирования и прогнозирования («Эсплан», «Император»).

Система CASCON построена на фазово-факторной модели Блумфильда-Лейсса, что позволяет ей быть экспертно-аналитической системой. Принцип работы рассматриваемого программного решения базируется на

разделении конфликтной ситуации (в данном случае террористической и экстремистской деятельности) на стадии (этапы), ввиду чего противоправные действия могут быть классифицированы в зависимости от степени напряженности.

CASCON разделяет каждый конфликт на несколько основных стадий:

1) Диспут (начальная стадия конфликта, вооруженного противодействия нет, либо оно слабо выражено);

2) Конфликт (активная фаза с ярко выраженным вооруженным противодействием, высокая социальная напряженность, переговоры с террористами не представляются возможными, либо не дали положительных результатов);

3) Прекращение конфликта (переговорная фаза после исчерпания вооруженных и иных ресурсов);

4) Урегулирование (решение проблем, приведших к конфликту).

АРИАДНА+ – система, построенная на применении искусственного интеллекта, позволяет анализировать и прогнозировать ситуации, возникающие в политической, экономической и социальной сферах жизни общества, поступающие и хранящиеся в специально созданном банке данных.

Источниками для поступления информации в системе АРИАДНА+ выступают открытые ресурсы сети Интернет, поскольку функциональный потенциал рассматриваемого программного решения базируется на семантическом и лингвистическом анализе.

АРИАДНА+ рассматривает террористическую и экстремистскую деятельность как совокупность институциональных актов противоправного характера, что позволяе правоохранительным и специальным органам нацелено осуществлять безопасность объектов от такого вида угроз.

«Мониторинг социальной напряженности» – экспертная система, разработанная Уральской академией государственной службы специально для администрации Ямало-Ненецкого автономного округа, в целях прогнозирования развития конфликтной ситуации, путем мониторинга определенных событий.

Информационными источниками для данной системы выступают опросы населения, которые после загрузки фильтруются инструментарием и анализируются. Несмотря на простоту задумки производителей, систему «Мониторинг социальной напряженности» нельзя назвать полноценным программным решением, предназначенным для противодействия терроризму и экстремизму, поскольку опросы – субъективная оценка населения на определенную возникшую ситуацию в обществе.

«Семантический архив» – информационно-аналитическая система общественной безопасности, базирующаяся на сборе информации из открытых источников и ее последующем анализе.

Процесс работы рассматриваемого программного решения можно условно разделить на 5 самостоятельных этапа:

1) Сбор информации;

2) Обработка информации (выделение смысловых конструкций, заданных шаблоном);

3) Запрос информации из шаблона;

4) Выделение смысловых цепочек в анализируемом тексте;

5) Формирование отчетной документации.

Системный комплекс «Тренд» – математический аппарат прогнозирования ситуации, путем расчета частоты использования конкретной персоной словесных конструкций и на основании полученных данных строить прогноз развития конфликта.

На сегодняшний день комплекс «Тренд» считается «сырым» информационным продуктом, поскольку практическое его применение показало 47% точность сбывания прогнозов системы.

Системы «Эсплан» и «Иматор» – системы поддержки принятия решений, позволяющие определять отношения между лицами и факторами, путем составления многоуровневой модели проблемы, которая выглядит следующим образом:

1 уровень – проблема, ее составляющие (причины, условия, факторы зарождения и развития);

2 уровень – субъекты конфликта и разрешения конфликта;

3 уровень – характеристики субъектов из 2 уровня (тип, ресурсы, количество);

4 уровень – построение возможных дальнейших сценариев конфликта.

«Эсплан» и «Император» позволяют строить прогнозы в зависимости от действий конкретных лиц, что в свою очередь, гарантирует реализацию грамотного подхода специальными органами для решения проблемы терроризма и экстремизма с минимальными потерями ресурсов и численного состава сотрудников и гражданского населения.

Таким образом, использование информационных технологий анализа, моделирования и прогнозирования позволит в существенной мере снизить временные расходы на поиск информации террористической и экстремистской направленности в различного рода источниках.

Практическая значимость проведенного исследования выражается в использовании его результатов в научной и учебной деятельности, с целью повышения компетентных навыков обучающихся по специальностям, связанных с информационной безопасностью и изучением информационных технологий.

Литература

1. https://it2b.ru/archive/3308/

2. Бельский В.Ю., Сацута А.И. Терроризм как социально – политическое явление. Противодействие в современных условиях: монография. – М.: ЮНИТИ – ДАНА, 2015. – 367 с.

3. Беляков А.А. Криминалистическое взрывоведение: проблемы теории и практики. Красноярск: Универс, 2015. С. 17.

4. Токмакова А.Х. Формы правления в современном мире / Молодежь и XXI век – 2016 Материалы VI Международной молодежной научной конференции. В 4-х томах. 2016. С. 96-99.

5. Тынымсеитова С.М. Форма правления государства сквозь призму историко – правовой мысли // Новая наука: От идеи к результату. 2017. Т. 1. № 3. С. 193-197.

Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошее, В. Черкасов. // Уголовное право. 2013. – № 3. – С. 9-11.

8. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014.- 182 с.

Ефимова Юлия Сергеевна,
преподаватель кафедры информационной безопасности
Краснодарского университета МВД России

ИСПОЛЬЗОВАНИЕ МЕТОДОВ OSINT В РАМКАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Одним из ключевых инструментов в борьбе с киберпреступностью является метод OSINT (Open Source Intelligence). Данный метод представляет собой процесс сбора информации из открытых источников и позволяет профессионалам в области кибербезопасности предсказывать, прослеживать и предотвращать киберпреступления, используя доступные публичные данные. Открытые источники могут включают в себя как публичные базы данных и веб-сайты, так и социальные сети, и форумы. Используя методы OSINT, специалисты по кибербезопасности могут собирать важные данные о потенциальных угрозах, а также прослеживать их действия в цифровом пространстве.

Как известно, киберпреступники используют интернет для планирования, организации и осуществления своих преступных действий. С помощью OSINT специалисты по кибербезопасности могут отслеживать подозрительную активность, анализировать методы и прогнозировать возможные атаки.

Специалисты по кибербезопасности могут использовать методы OSINT для:

- Профилирования киберпреступников: OSINT может быть использован для сбора информации о подозреваемых, включая их поведение в интернете, используемые сети и инструменты, а также связи с другими преступниками.
- Анализа технической информации: это может включать в себя анализ IP-адресов, доменных имен, метаданных, кода и другой технической информации, которая может помочь в расследовании.
- Отслеживания киберпреступных групп: OSINT также может быть использован для мониторинга активности киберпреступных групп, их обсуждений, планов и методов атаки.

Инструменты и сервисы для OSINT.

При проведении OSINT-анализа специалисты по кибербезопасности используют различные инструменты и сервисы. Ниже представлены некоторые из них:

1. **Shodan**: Этот поисковик используется для поиска различных типов устройств, подключенных к интернету, от веб-камер до промышленных систем управления.
2. **Maltego**: Программа для сбора данных и визуализации связей между объектами. Позволяет создавать детализированные графы для различных типов данных и устанавливать связи между ними.

3. **theHarvester**: Инструмент для сбора информации о домене или компании. Может извлекать данные из поисковых систем, PGP-ключевых серверов, баз данных WHOIS и других источников.

4. **Google Dorks**: Специальные запросы к поисковой системе Google, которые позволяют находить информацию, скрытую от обычного поиска.

5. **Recon-ng**: Полноценная оболочка с интерфейсом, похожим на Metasploit. Разработана для веб-рекогниции и может быть использована для сбора информации о компаниях, людях, сайтах и т. д.

6. **Tineye**: Сервис для обратного поиска изображений. Позволяет находить все варианты использования конкретного изображения в интернете.

7. **Social Searcher**: Бесплатный сервис, который позволяет быстро искать информацию в различных социальных сетях.

8. **WHOIS**: Сервис, позволяющий получить информацию о владельце домена, включая имя, местоположение, контактные данные и другую информацию.

Использование OSINT в контексте кибербезопасности и противодействия киберпреступности предоставляет огромные возможности для мониторинга, анализа и предупреждения потенциальных угроз. При правильном использовании, методы OSINT могут значительно повысить эффективность работы специалистов по кибербезопасности, позволяя лучше понимать угрозы и принимать своевременные меры для их предотвращения.

Однако, необходимо помнить, что OSINT — это лишь один из инструментов в арсенале специалиста по кибербезопасности. Для обеспечения наиболее полной и эффективной защиты, он должен быть использован в сочетании с другими методами и подходами, включая защиту периметра, использование антивирусного программного обеспечения, обучение сотрудников и многое другое.

В заключение, стоит отметить, что важность OSINT будет продолжать расти с увеличением объема доступной публичной информации и усовершенствованием инструментов и методов ее анализа. Поэтому освоение навыков работы с OSINT будет полезным для любого специалиста в области кибербезопасности.

Кобец Петр Николаевич,
доктор юридических наук, профессор
главный научный сотрудник
Центра организационного обеспечения научной деятельности
Всероссийского научно-исследовательского института МВД России

О ВАЖНОСТИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ РОССИЙСКОГО ОБЩЕСТВА

Освещая проблематику противодействия информационному терроризму сразу же необходимо указать на то, что, с целью минимизации различных рисков, связанных преступными посягательствами, совершаемыми с использованием информационных технологий, Президентом Российской Федерации В.В. Путиным на регулярной основе выдвигаются предложения, по объединению усилий мирового сообщества для совместной деятельности по обеспечению информационной безопасности[1].

28 февраля 2023 г. выступая на ежегодной расширенной коллегии Федеральной службы безопасности Российской Федерации В.В. Путин отметил, что по-прежнему актуальная задача – противодействие террористической угрозе, поскольку за прошедший год количество подобных преступлений выросло. По большей части по мнению Президента Российской Федерации это связано и с попытками киевского режима использовать методы террора, а также со стремлением Запада реанимировать ячейки экстремистов и террористов, на нашей территории. Кроме того, Президент Российской Федерации В.В. Путин указал на необходимость «и дальше повышать уровень защищенности информационного, цифрового пространства Российской Федерации, выявлять и пресекать попытки нарушить работу российских ресурсов и коммуникаций»[2].

Оценивая опасность информационного терроризма Министр внутренних дел Российской Федерации генерал полиции Российской Федерации В.А. Колокольцев, также неоднократно отмечал, что угроза проведения террористических актов в Российской Федерации осуществляется международными террористическими организациями при помощи компьютерных программ спам-ботов, с целью посеять в российском обществе чувство страха и

---

[1] Кобец П.Н. Роль Президента Российской Федерации В.В. Путина в объединении усилий мирового сообщества по совершенствованию информационной безопасности в киберпространстве // Правопорядок: история, теория, практика. – 2022. – № 2(33). – С. 62-68. С. 65.

[2] Заседание коллегии ФСБ России [Электронный ресурс] // UPL: http://www.kremlin.ru/events/president/news/70597 (дата обращения 09.03.2023).

незащищенности, а также дезорганизации работы различных организаций в нашей стране[1].

В результате научно-технической революции при помощи информационных технологий совершается большинство видов преступных посягательств, в том числе и различные акты терроризма[2]. Особая значимость рассматриваемой проблемы выражается в том, что современное цифровое общество испытывает массу различных затруднений и неприятностей от неспособности правоохранителей остановить волну данной преступности. Так что актуальность и важность проведения исследований, направленных на повышение борьбы с рассматриваемыми преступными посягательствами абсолютно бесспорна, поскольку полученные в результате научной проработки различных вопросов, а также выводы и рекомендации позволят в дальнейшем правоохранителям грамотно и результативно противодействовать всем проявлениям информационного терроризма[3].

В этой связи следует отметить, что немаловажное значение в рассматриваемом контексте имеет обстоятельство, в следствии которого, на сегодняшний день отсутствует единый научный и обоснованный подход в понимании самого феномена противодействия рассматриваемому террору[4]. Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности «понятие информационного террора трактует очень широко, определяя его, как использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях»[5].

---

[1] Колокольцев: телефонные террористы звонят из-за рубежа с помощью компьютерных программ [Электронный ресурс] // UPL: https://tass.ru/proisshestviya/4706403 (дата обращения 09.03.2023).

[2] Кобец П.Н. Криминологические проблемы борьбы с преступлениями, совершаемыми с использованием современных информационных технологий // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: Материалы международной научно-практической конференции, Москва, 02–03 декабря 2021 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2022. – С. 58-62. С. 59.

[3] Панталева Н.С., Пархитько Н.П. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. – 2019. – № 3. – С. 47-50. С. 48.

[4] Кобец П.Н. Анализ практики возникновения, становления и активного применения методов информационно-психологического противоборства // Юридическая психология. – 2022. – № 2. – С. 37-40. – DOI 10.18572/2071-1204-2022-2-37-40. С. 38.

[5] «Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» (Екатеринбург, 16 июня 2009 г. [Электронный ресурс] // UPL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#004833319880921527 (дата обращения 09.03.2023).

Признаками информтерроризма являются «использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы»[1].

Хотелось особо указать на то, что по мнению отечественных исследователей, и с этим трудно не согласиться целью борьбы с информационным терроризмом является осуществление комплекса мер, направленных на защиту личности общества и государства от угроз, и проявлений терроризма в информационном пространстве поскольку, «распространяя террористические идеи**,** субъекты террористской деятельности стремятся к максимальному использованию информационного пространства, которое в современном информационном обществе обладает более широкими возможностями для этих целей, и состоит из информационных субъектов, которые могут создавать, накапливать и передавать информационные данные, а в качестве таких субъектов могут выступать люди, социальные группы, корпорации, государственные органы»[2], одним словом все использующие возможность информтехнологий.

Изучение различных источников юридической литературы позволяет утверждать о том, что «под противодействием информационному терроризму следует понимать информационное, идеологическое, правовое, организационное и иное воздействие, которое направленно на воспрепятствование информационно-психологическим атакам террористических организаций и отдельных террористов, нацеленных и осуществляемых против личности, общества и государства»[3]. Авторское понимание данной дефиниции, связанной с противодействием информтерроризму в первую очередь основывается на расширенном подходе к борьбе с рассматриваемым противоправным явлением, кроме того оно специально ориентировано на то чтобы

---

[1] Сидненко Г.Ф. Государственная политика Российской Федерации в области информационного противодействия терроризму // Современное право. – 2015. – № 4. – С. 106-113. С. 112.

[2] Есаулов В.Т. Противодействие информационным угрозам как важное направление политики национальной безопасности Российской Федерации // Власть. – 2009. – № 12. – С. 69-72. С. 70.

[3] Кобец П.Н. Информационное воздействие как один из современных методов терроризма и меры борьбы с ним // Вестник Краснодарского университета МВД России. – 2022. – № 1(55). – С. 10-14. С. 11.

была возможность устранения основных факторов, которые способствуют складывающимся в информационном пространстве вызовам безопасности[1].

При этом важно отметить, что информационное пространство является довольно специфической средой. В нем происходит изменение содержательной части ряда понятий, таких, как силовое противоборство, информационно-психологическое противоборство, вооруженная борьба и др.[2] Опыт борьбы с информационным терроризмом дает основание утверждать о том, что использование силовых методов по борьбе с ним, может способствовать тому, что на какое-то время конкретная угроза совершения террористического акта может быть локализована. Однако общая «угроза информационному пространству не исчезнет до тех пор, пока функционирует система по воспроизводству инфраструктуры террора, а ключевое звено данной системы – террористическая идеология, и кроме того источники и каналы по которым происходит ее распространение»[3].

Соответственно, в первую очередь основные усилия, сосредоточенные государством в лице правоохранителей на противодействии информационному терроризму, должны быть направлены на борьбу с вышеуказанными ключевыми звеньями, а уже потом на террористические организации, общественные объединения, террористическое подполье, информационная террористическая деятельность которых в конечном итоге сводиться к подрыву безопасности нашей странны[4]. Как отмечают отечественные эксперты в сфере борьбы с вербовочной деятельностью международных террористов в телекоммуникационном и информационном пространке, по уровню организации, подготовки и воздействия, информационно-психологические террористические операции могут быть стратегическими, оперативными и тактическими. При этом пропаганда рассматривается идеологами терроризма, в

---

[1] Хохлов Н.И., Шамигулов А.Р., Бахарев В.М. Информационная система и её роль в формировании гражданской идентичности по противодействию идеологии терроризма в молодежной среде // Социально-ориентированное проектирование системы формирования гражданской идентичности учащейся молодежи в поликультурном образовательном пространстве: Сборник материалов Международной научно-практической конференции, Казань, 28 февраля 2018 года. Том 2. – Казань: Издательство «Данис», 2018. – С. 207-214 С. 212..

[2] Кобец П.Н. Совершенствование межгосударственного сотрудничества в сфере информационной безопасности: основа противодействия международной киберпреступности // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 1. – С. 83-89. С. 85.

[3] Щербакова А.В. Взаимосвязь информационных технологий и терроризма XII Международный молодежный форум «Образование. Наука. Производство»: Материалы форума, Белгород, 01–20 октября 2020 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2020. – С. 2050-2053. С. 2052.

[4] Кобец П.Н. Основы обеспечения национальной экономической безопасности от новейших угроз киберпреступности // Научное обозрение: теория и практика. – 2022. – Т. 12, № 3(91). – С. 426-434. – DOI 10.35679/2226-0226-2022-12-3-426-434. С. 426.

качестве систематического, целенаправленного распространения при помощи СМИ, конкретных положений в целях воздействия на мнение, чувство, состояние и отношение либо поведение объекта воздействия, для достижения прямой, либо косвенной выгоды для террористической организации[1].

Поэтому важно указать на то, что в современных условиях борьба с рассматриваемым видом террористической угрозы является особым видом деятельности, которая осуществляется субъектами борьбы с терроризмом. Кроме того, она включает в себя как само выявление основных детерминант данного явления, так и дальнейшее устранение основных причин и условий, которые способствуют совершению рассматриваемых террористических угроз[2].

Кроме того, информационный терроризм в качестве одного из важнейших методов террористической деятельности, активно практикуется террористами для рекрутинга новых сторонников терроризма и психологическому воздействию на лиц, уже вступивших в ряды террористов[3]. Поэтому среди наиболее значимых факторов, влияющих на развитие рассматриваемой террористической угрозы, выступает использование террористическими организациями методов информационного противоборства, основанных на информационно-коммуникационных технологиях.

Сегодня совершенно очевидно, что, без регулярного и планового обновления всей правовой среды в области совершенствования отечественного уголовного законодательства, направленного на противодействие информационному террору, чрезвычайно сложно бороться с глобальными угрозами в данной сфере[4].

В этой связи немаловажно и то, что совершенствование организационных и тактических направлений работы по противодействию информационным террористических угрозам должно основываться на передовых отечественных и зарубежных теорий, и практик, технических и технологических новшеств, и в первую очередь связанных с программным обеспечением, используемым в деятельности МВД России[5]. В том числе помимо совершен-

---

[1] Сундиев И.Ю. Противодействие вербовочной деятельности международных террористических организаций в сети интернет // Научный портал МВД России. – 2017. – № 2(38). – С. 89-95. С. 91.

[2] Сидненко Г.Ф. Научные подходы к оценке эффективности реализации государственной политики в области информационного противодействия терроризму // Современное право. – 2015. – № 5. – С. 114-118. С. 115.

[3] Сидненко Г.Ф., Ахмедов В.Х. Информационное противодействие терроризму в Российской Федерации: понятийно-содержательный анализ // Мир образования – образование в мире. – 2015. – № 3(59). – С. 101-110. Ч. 105.

[4] Романенко И.И., Чепарова Н.В. Особенности профилактики экстремизма и терроризма в России на современном этапе // Право. Экономика. Безопасность. – 2017. – № 3(11). – С. 82-85. С. 83.

[5] Таова Л.Ю. Основные направления противодействия актам терроризма // Пробелы в российском законодательстве. – 2020. – Т. 13, № 4. – С. 83-86. С. 85.

ствования программного обеспечения и нормативно-правовой базы по организации борьбы с терроризмом в информационной сфере, следовало бы изучить и проработать вопрос о необходимости расширения полномочий отдельных субъектов ОВД по борьбе с информационным терроризмом.

Поскольку использование цифровых технологий с каждым днем становится неотъемлемую часть жизнедеятельности современного общества, необходимо создание эффективной и действующей правовой среды, в которой размещались бы самые последние цифровые продукты и услуги в сфере осуществления безопасности в информационном пространстве, при этом данная деятельность должна способствовать тотальному контролю всех технологических процедур в области высоких технологий, а этого невозможно добиться без совершенствования программного обеспечения борьбы с рассматриваемыми проявлениями.

Кроме всего прочего, важно отметить, что оказывать грамотное противодействие всем явлениям, связанным с большинства преступных посягательств в области информационного терроризма, с каждым годом осложняющих работу всех отечественных правоохранителей следует исключительно на плановой основе, при этом также нужно вводить прогнозирование дальнейшей криминальной ситуации в рассматриваемой сфере, чтобы правоохранители смогли во всеоружии противостоять рассматриваемым преступлениям[1].

Помимо вышеперечисленных условий эффективного противодействия рассматриваемому виду террористической угрозы, информационные террористические атаки требуют от правоохранителей, которые им противодействуют обрабатывать большой информационный массив и прибегать к адекватным решениям в течении короткого временного промежутка. Подобный подход к борьбе с информационным терроризмом также требует от правоохранителей постоянно разрабатывать, выявлять, оперативно реагировать и предупреждать информационные террористические угрозы, и непременно осуществлять внедрение положительного опыта в аналогичные структурные подразделения.

В заключении важно отметить, что решать задачи борьбы с проявлениями информационного терроризма, которые совершаются с использованием информационных технологий, практически невозможно сложно без реализации мер по активной научной поддержке, и внедрения в практику современных научных разработок, в том числе и необходимого программного обеспечения, подготовленного специалистами научных и образовательных учреждений органов внутренних дел.

---

[1] Сидненко Г.Ф. О национальной стратегии информационного противодействия терроризму // Вестник Московского государственного лингвистического университета. Общественные науки. – 2019. – № 4(837). – С. 64-76. С. 71.

Назаров Артур Карапетович,
преподаватель кафедры информационной безопасности
Краснодарского университета МВД России,
кандидат физико-математических наук

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ФАКТОР РАЗВИТИЯ КИБЕРПРОСТРАНСТВА

На современном этапе развития информационных технологий одним из важнейших факторов развития киберпространства несомненно является быстрое развитие искусственного интеллекта и его внедрение как в средства атаки, так и как средства защиты информации. Это приводит к качественным изменениям в сфере кибербезопасности.

Так, например, мошенники все чаще стали использовать искусственный интеллект и машинное обучение в чат-ботах для создания так называемых «идеальных текстов», устранив при этом основной недостаток фишинговых атак – «некачественный» текст. Искусственному интеллекту лучше, чем злоумышленнику удается написать текст, внушающий доверие. Вследствие чего получатели таких сообщений стали чаще переходить по распространяемым в подобных сообщениях вредоносным ссылкам. Также с помощью таких чат-ботов злоумышленникам стало проще распространять различные виды вредоносных программ. Другим вектором развития является их внедрение в легитимные чат-боты посредством взлома последних. В дальнейшем такие чат-боты совершают кибератаки на клиентов взломанного чат-бота, пытаются получить от них личную или конфиденциальную информацию. Существуют также чат-боты, которые имитируют человека. Так, чат-боты, маскирующиеся под человека определенного пола, внедряются на сайты знакомств для выманивания важной информации от других пользователей. Еще одним направлением использования искусственного интеллекта злоумышленниками можно считать создание вредоносного программного кода.

Некоторые злоумышленники также используют несовершенство искусственного интеллекта и путем создания особых запросов обходят защиту разработчиков искусственного интеллекта и получают «опасную информацию», которую они могут в дальнейшем использовать в своих целях.

Так как искусственный интеллект как правило тесно взаимодействует с пользователями, то он содержит в себе большой массив данных о нем. На основе этих данных может быть создано досье на человека. Потому потенциальная возможность утечки такой информации также следует отнести к угрозам использования искусственного интеллекта.

Искусственный интеллект в руках злоумышленников может оказаться мощным оружием, например, инструментом для создания фишинговых сай-

тов, сетевых атак, обхода различных средств защиты информации, для создания фейковых новостей, дезинформации и т.д. Этот список можно продолжать и дальше.

Несомненно, искусственный интеллект на сегодняшний день – это мощный инструмент в руках человека. Наряду с большой угрозой, которую несет в себе искусственный интеллект, он также несет в себе и большую ценность, в частности, как средство защиты. Так, например, для противодействия искусственному интеллекту, создающему фишинговые сайты и распространяющему письма с фишинговыми ссылками, необходимо создание искусственного интеллекта, анализирующего содержание входящих писем. Такая система должна обрабатывать все письма до предоставления к ним доступа пользователям. На основе, имеющихся у него шаблонов, система должна научиться отличать (по структуре) фишинговые ссылки от обычных, отличать обычных отправителей от злоумышленников и ботов (например, на основе имеющихся баз данных электронных почт известных компаний, списков доверенных электронных почт и электронных почт и писем, используемых ранее злоумышленниками). При этом такая система должна постоянно совершенствоваться, обучаться на основе новых данных и шаблонов. Аналогичным способом каждой системе с искусственным интеллектом, совершающей вредоносные действия, должна быть поставлена в соответствие другая система с искусственным интеллектом, противодействующая ей. Такой поход позволить нивелировать угрозы, исходящие от искусственного интеллекта – «обоюдоострого меча», используемого для нападения и защиты от киберпреступников.

Литература

1. Н. Хауз. Полный курс по кибербезопасности: секреты хакеров. Т. 1 / Н. Хауз 2017. – 271 с.

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

Назмеева Лейсан Рафиковна,
кандидат экономических наук,
старший преподаватель кафедры экономики,
финансового права и информационных технологий
в деятельности органов внутренних дел
Казанского юридического института МВД России

Каримов Фидаиль Ирекович,
курсант Казанского юридического института МВД России

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА: ОСНОВНЫЕ НАПРАВЛЕНИЯ ВЫЯВЛЕНИЯ И РАСКРЫТИЯ

Стремительное развитие информационной среды выступает одним из приоритетных направлений внутренней и внешней политики Российской Федерации[1], направленных на реализацию революционного процесса информатизации во всех сферах жизнедеятельности общества и становлению информационного общества. Внедрение информационно-телекоммуникационных технологий способствует возникновению новых более выгодных альтернатив в финансово-кредитной сфере и обусловливает использование безналичных денежных средств в электронной коммерции, а также предопределяет становление электронных средства платежа в качестве универсального средства урегулирования различных обязательств возмездного характера постепенно вытесняя традиционный оборот с наличными денежными средствами.

По данным Банка России прослеживается увеличение доли безналичных операций, характеризующихся концентрацией и движением денежных средств с помощью электронных платежных систем и с использованием расчетных (дебетовых) и кредитных карт, эмитированных российскими кредитными организациями и Банком России (количество переводов денежных средств в 2020 г. – 1844, 2021 г. – 2643, 2022 г. – 4958[2]).

С активным распространением дистанционного банковского обслуживания возросло количество общественно-опасных деяний, квалифицируемых как мошенничество с использованием электронных средств платежа (статья 159.3 Уголовного кодекса Российской Федерации[3]).

---

[1] Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы: указ Президента РФ от 09 мая 2017 г. № 203 // Собрание законодательства РФ. – 2017. – 15 мая.

[2] Статистика национальной платежной системы URL: https://www.cbr.ru/statistics/nps/psrf/ (дата обращения: 12.04.2023)

[3] Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собрание законодательства Российской Федерации. – 1996. – 17 июня

Согласно статистическим данным Министерства внутренних дел Российской Федерации количество мошенничеств с использованием электронных средств платежа в 2019 году составило 16 119, что на 280% больше чем за аналогичный период предыдущего года, в 2020 г. – 25 820 (+60,2%)., 2021 г. – 1-258 (-60,3%), в 2022 г. – 7288 (-29%)[1].

Мошеннические действия рассматриваемого вида выступают преступлением новой формации, совершаемым дистанционным и бесконтактным способом[2] в условиях постепенной интеграции всех видов телекоммуникационных и информационных услуг в рамках единого информационного пространства, тем самым обуславливая трансформацию способов и методов хищения денежных средств.

По мнению научных специалистов, к данным преступлениям следует относить мошенничество в онлайн формате (например, хищение или неправомерное использование личных учетных данных, информация о банковской карте; фишинг и спуфинг-атаки) и традиционное мошенничество в офлайн формате (например, завладение обманным путем по телефону или с использованием почты)[3].

Анализ правоприменительной практики свидетельствует о высоком уровне совершения мошенничества с использованием банковских карт, системы «Клиент-Банк», а также систем «Яндекс.Деньги», «QIWI-кошелек» и «WebMoney».[4] Так, например, активное распространение получило осуществление звонков лицам через популярные мессенджеры «What’s App», «Telegram» с использованием логотипа сервиса «Госуслуги» или кредитной организации, направленных на введение в заблуждение в целях завладения конфиденциальной информации и хищения денежных средств[5].

---

[1] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 14.04.2023).

[2] Новоселов Н.Г., Чиненов А.В. О некоторых вопросах раскрытия мошенничеств, совершаемых с использованием банковских карт // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2019. – № 3. – С. 24-28.

[3] Бачиева А.В., Бозиев Т.О. Уголовно-правовая и криминалистическая характеристики мошенничества с использованием электронных средств платежа// Журнал правовых и экономических исследований. – 2022. – № 2. – С. 7-12.

[4] Малянова К.П. Актуальные проблемы в деятельности правоохранительных органов при выявлении и раскрытии преступлений с использованием электронных средств платежа// Юристъ-Правоведъ. – 2021. – № 2(97). – С. 148-150.

[5] Мошенники начали звонить зеленодольцам через мессенджеры. URL: https://16.xn--b1aew.xn--p1ai/news/item/35764993/ (дата обращения 20.02.2023).

Механизм совершения противоправного деяния рассматриваемого вида обладает определенной спецификой, обусловленной наличием технологии дистанционной передачи данных с использованием коммуникационных сетей[1].

В условиях активного использования в противоправных целях всего спектра технологий и инструментов, обуславливающий отсутствие внесения изменений алгоритма следообразования во внешнюю среду особую значимость приобретает выработка специальных способов выявления и раскрытия сотрудниками органов внутренних дел мошенничества с использованием электронных средств платежа.

Обратим внимание, что при совершении рассматриваемого преступления применяются способы хищения, отражающие минимальное количество криминалистически значимой информации[2] и в целях действенного собирания доказательственной базы представляется целесообразным рассмотреть вопрос о включении на первоначальном этапе расследования преступления при поступлении информации о факте совершения мошенничества с использованием электронных средств платежа в состав следственно-оперативной группы сотрудников отдела уголовного розыска, обладающих специальными знаниями и техническими навыками в раскрытии рассматриваемых преступлений, предварительно прошедших профессиональное обучение в данном направлении.

В целях эффективности использования дополнительных сил и средств органов внутренних дел по борьбе с рассматриваемыми преступлениями важное значение приобретает организация деятельности органов внутренних дел в виде действенности и последовательности действий. С учетом данного обстоятельства особую роль приобретает разработка сотрудниками Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, Управления уголовного розыска и контрольно-методическим подразделением следственных органов территориальных органов МВД России на региональном уровне с последующим внедрением частных и общих методик расследования мошенничества с использованием электронных средств платежа (например, установление алгоритма действий сотрудников органов внутренних при поступлении сообщения о совершенном преступлении, первоначальных

---

[1] Малянова, К.П. Актуальные проблемы в деятельности правоохранительных органов при выявлении и раскрытии преступлений с использованием электронных средств платежа // Юристъ-Правоведъ. – 2021. – № 2(97). – С. 148-150.

[2] Стромова К.В. Актуальные проблемы расследования преступлений, связанных с мошенничеством // Тамбовские правовые чтения имени Ф.Н. Плевако: Материалы III Международной научно-практической конференции. В 2-х томах, Тамбов, 24–25 мая 2019 года / Ответственный редактор В.Ю. Стромов. Том 1. – Тамбов: Издательский дом «Державинский», 2019. – С. 422-426.

действиях в целях собирания следов преступления и формирования доказательственной базы) или методических рекомендаций об организации служебной деятельности по взаимодействию с иными подразделениями в ходе раскрытия и расследования преступлений[1].

Результативность получения обширного круга доказательственной информации, способствующей действенной реализации вопросов выявления и раскрытия данного вида преступления, во многом зависит от действий сотрудников органов внутренних дел в ходе осмотра места происшествия и полного проведения комплекса оперативно-розыскных мероприятий.

Учитывая, что осмотр места происшествия выступает отправной точкой для получения сведений, необходимых для выдвижения следственных версий и собирания доказательств о совершенном преступлении, представляется целесообразным:

- осмотр технических устройств проводить с участием специалистов, имеющих познания в данной области. Например, знания специалиста способствуют сохранению контактов в момент изъятия при демонтаже посторонних устройств на банкомате, сведения об IP-адресах, с которых производится администрирование интернет-сайта, доменного имени и/или IP-адреса, выявление сторонних заходов. В зависимости от условий совершения общественно-опасного деяния в качестве специалистов рекомендуется приглашать сотрудников технического отдела банка, которые непосредственно занимались установкой и обслуживанием терминала[2]. В случаях выявления факта функционирования Интернет – ресурса, с использованием которого совершено преступление необходимо установить и документально отразить сведения о данном сайте адресную строку и идентификатор страницы, использовать фото- и видеофиксацию [3];

– осмотр персонального компьютера и смартфона, планшета, ноутбука следует проводить с участием специалиста с целью сохранения следов и механизма совершения преступления, установления алгоритма преступного действия (например, отключение от сети Интернет и удаленного доступа к техническому устройству путем включения авиарежима).

---

[1] Ильяш А.В. Понятие, виды и содержание деятельности контрольно-методических подразделений следственных органов территориальных органов МВД России на региональном уровне // Труды Академии управления МВД России. – 2014. – № 4(32). – С. 106-109.

[2] Лозовский Д.Н Лозовская Н.Н., Ульянова И.Р. Особенности производства осмотра места происшествия при расследовании преступлений, совершенных с использованием банковских карт // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 10. – С. 163-165.

[3] Семенихина Т.Н. О проведения осмотра места происшествия при проверке заявления (сообщения) о дистанционном мошенничестве // Гуманитарные, социально-экономические и общественные науки. 2020. №7. С.184 – 186.

При совершении оперативно-розыскных мероприятий, направленных на сбор информации и формирования действенных направлений раскрытия рассматриваемых общественно –опасных деяний представляется необходимым:

− осуществлять опрос заявителя, работников банка, имеющих доступ к охраняемой законом тайне о банковских счетах, персональных данных клиентов банка, в чьи обязанности входит осуществление банковских операций в целях установления источника получения платежной карты, способа обналичивания денежных средств, местонахождения оборудования, похищенных денежных средств.

− изучать информацию о способе совершения и сокрытии преступления, включающее в себя особенности подготовки, совершения и сокрытия общественно-опасного деяния в целях исследования влияния данных о деятельности преступника в окружающей среде, и восстановления механизма преступного поведения.

Особую значимость представляет осуществление взаимодействия следственных и оперативно-розыскных подразделений органов внутренних дел, реализовывающееся путем:

– проведения совместного анализа материалов уголовного дела[1] в целях установления возможных пробелов в планировании или производстве следственных действий, координации дальнейших действий по раскрытию преступлений с учетом всех необходимых форм, сил и средств;

– активного использования оперативно-справочных, розыскных, криминалистических учетов и иных учетов, которые могут содержать сведения, имеющие отношение к расследуемому преступлению;

– составления, своевременного обновления и корректирования развернутого плана совместной работы с учетом разнообразных версий.

В условиях трансформации преступности и проявлении новых схем совершения мошенничества с использованием электронных средств платежа представляется целесообразным осуществлять повышение квалификации сотрудников органов внутренних дел, специализирующихся на выявлении, раскрытии и расследовании преступлений, в целях обучения, ориентированного на выстраивание целенаправленной системы противодействия подобным преступлениям.

В подобных условиях возрастает необходимость проведения обучающих занятий совместно с представителями Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий, Банка России, специалистами ведущих IT-компаний России, направленных на рассмотрение современных тенденций цифровизации

---

[1] Имаева Ю.Б. К некоторым вопросам повышения эффективности деятельности следователя по приостановленым производством уголовным делам о хищениях с использованием банковских карт и их реквизитов // Правовое государство: теория и практика. – 2014. – № 3(37). – С. 88-91.

различных сфер деятельности, видов киберпреступлений, выявление особенностей способов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и т.д.

Таким образом, эффективность противодействия мошенничеству с использованием электронных средств платежа проявляется путем профессиональных действий сотрудников органов внутренних дел при осмотре места происшествия и своевременном, полном проведении комплекса следственных и оперативно – розыскных мероприятий, а также сформированной культуры использования инструментария раскрытия преступления, направленного на защиту интересов общества и государства.

Литература

1. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собрание законодательства Российской Федерации. – 1996. – 17 июня

2. Бачиева А.В., Бозиев Т.О. Уголовно-правовая и криминалистическая характеристики мошенничества с использованием электронных средств платежа// Журнал правовых и экономических исследований. – 2022. – № 2. – С. 7–12.

3. Ильяш А.В. Понятие, виды и содержание деятельности контрольно-методических подразделений следственных органов территориальных органов МВД России на региональном уровне / А. В. Ильяш // Труды Академии управления МВД России. – 2014. – № 4(32). – С. 106-109. – EDN WEIYLP.

4. Имаева Ю.Б. К некоторым вопросам повышения эффективности деятельности следователя по приостановленым производством уголовным делам о хищениях с использованием банковских карт и их реквизитов // Правовое государство: теория и практика. – 2014. – № 3(37). – С. 88–91.

5. Лозовский Д.Н., Лозовская Н.Н., Ульянова И.Р. Особенности производства осмотра места происшествия при расследовании преступлений, совершенных с использованием банковских карт // Гуманитарные, социально-экономические и общественные науки. – 2018. – № 10. – С. 163–165.

6. Малянова К.П. Актуальные проблемы в деятельности правоохранительных органов при выявлении и раскрытии преступлений с использованием электронных средств платежа // Юристъ-Правоведъ. – 2021. – № 2(97). – С. 148–150.

7. Мошенники начали звонить зеленодольцам через мессенджеры. URL: https://16.xn--b1aew.xn--p1ai/news/item/35764993/ (дата обращения 20.02.2023).

8. Новоселов Н.Г., Чиненов А.В. О некоторых вопросах раскрытия мошенничеств, совершаемых с использованием банковских карт // Вестник

Белгородского юридического института МВД России имени И.Д. Путилина. – 2019. – № 3. – С. 24–28.

9. Семенихина Т.Н. О проведения осмотра места происшествия при проверке заявления (сообщения) о дистанционном мошенничестве // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 7. – С. 184–186.

10. Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 14.04.2023).

11. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы: указ Президента РФ от 09 мая 2017 г. № 203 // Собрание законодательства РФ. – 2017. – 15 мая

12. Статистика национальной платежной системы. URL: https://www.cbr.ru/statistics/nps/psrf/ (дата обращения: 12.04.2023).

13. Стромова К.В. Актуальные проблемы расследования преступлений, связанных с мошенничеством // Тамбовские правовые чтения имени Ф.Н. Плевако: Материалы III Международной научно-практической конференции. В 2-х томах, Тамбов, 24–25 мая 2019 года / Ответственный редактор В.Ю. Стромов. Том 1. – Тамбов: Издательский дом «Державинский», 2019. – С. 422–426.

Осинцева Людмила Михайловна,
преподаватель кафедры информатики и специальной техники
Барнаульского юридического института МВД России

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Аннотация: В данной статье рассматриваются проблемы, касающиеся противодействия преступлениям в сфере информационно-коммуникационных систем инфраструктуры. Предложены возможные варианты их решения.

Ключевые слова: информационные системы, кибербезопасность, защита, вирусы, фишинг, стабильность, пользователи, санкции.

Сегодня для поддержания экономической стабильности общества и бесперебойного функционирования государства нужна надежная защита важнейших информационных систем общего пользования. Преступления, которые связаны с незаконным доступом к компьютерной информации, несут большую общественную опасность, так как компьютерная преступность является настоящим «бичом» экономики развитых государств.

В современном мире компьютерная безопасность (кибербезопасность) является стратегической проблемой государства, которая в комплексе затрагивает как экономику страны, так и совместную работу общенациональных производителей оборудования, комплектующих к нему, а также программного обеспечения для обеспечения бесперебойного обеспечения информационно-коммуникационных систем инфраструктуры. Сегодня из-за слабой рыночной конкурентоспособности уровень информационной защищённости в России пока находится на низком уровне, так как приходится пользоваться решениями иностранных производителей, а это не безопасно.

Кибербезопасность – «меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет). Поле деятельности системных администраторов охватывает все процессы и механизмы, с помощью которых цифровое оборудование, информационное поле и услуги защищаются от случайного или несанкционированного доступа, изменения или уничтожения данных, и приобретает всё большее значение в связи с растущей зависимостью от компьютерных систем в развитом сообществе» [1].

К основным категориям компьютерной безопасности можно отнести: «безопасность сетей (целевые атаки, вредоносные программы); безопасность приложений (угрозы, спрятанные в программах); безопасность информации (угроза целостности и приватности данных, как во время хранения, так и при передаче); операционная безопасность (полное или частичное разрушение операционной системы); аварийное восстановление и непрерыв-

ность бизнеса (реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных)» [2].

Факторы, которые негативно влияют на безопасную работу информационно-коммуникационных систем: кибератаки, разработка вирусов, спам, фишинг[1], троянские кони, атаки программ-вымогателей и др. Все это говорит о том, что современное общество очень зависит от стабильной работы информационных систем общего пользования.

Данные Министерства внутренних дел Российской Федерации на конец января 2023 года говорят о том, что показатели киберпреступлений в целом остаются стабильными. С использованием компьютерных современных технологий совершается каждое четвертое преступление.

В 2022 году количество преступлений в сфере компьютерной безопасности превысило планку в 523 тысячи – рост на 0,8% по сравнению с аналогичным периодом 2021 года. Три четверти подобных преступлений совершается с использованием Интернета, более трети (40,8%) – средства мобильной связи.

Заместитель председателя правительства Российской Федерации на встрече с президентом России Владимиром Путиным сообщил, что «в 2023 году число кибератак увеличилось на 80%. Основной целью хакеров был госсектор, российские специалисты ликвидировали более 25 тысяч кибератак на госресурсы и 1200 — на критическую инфраструктуру. Также он добавил, что против России воюют кибервойска всех недружественных стран и эта борьба будет продолжаться» [3].

В очередной раз президент США поддержал ряд санкций в отношении технической и инновационной отраслей, наложив запрет на экспорт полупроводников, компьютеров, сенсоров, лазеров и др. в Российскую Федерацию. В результате чего, российский власти при участии Минцифры предложили легализовать пиратское программное обеспечение. Что предполагало, за установку и использование этих продуктов пользователям не будет грозить наказание. Но позднее эту версию опровергли, заявив что министерство не вносило предложений по освобождению от ответственности за использование нелицензионного софта, и в настоящий момент не поддерживает их, а также планирует провести обсуждение с Минэкономразвития этого вопроса [4]. Должностные лица, отметили, что в первую очередь выступают за стимулирование россиян к переходу на отечественное программное обеспечение.

Представители данной отрасли сошлись во мнении, что на данный момент всё зависит от того, какую позицию займет компания Microsoft в дальнейшем. Большие проблемы могут начаться позже, когда множеству установленных приложений потребуется обновление операционной системы для

---

[1] Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логины, пароли).

дальнейшей бесперебойной работы, которое возможно будет получить только нелегально, либо стоит рассмотреть переход на операционную систему Linux. Российский эксперты по данной отрасли в один голос заявляют, что сегодня реально Microsoft заменить российскими сервисами. Более того для некоторых разработчиков ситуация может стать отличной возможностью занять освободившуюся нишу.

Основная масса успешных кибератак направлена на компьютеры, а также серверы конечных пользователей, подключенных к глобальной Интернет-сети. Поэтому на сегодняшний день обеспечение компьютерной безопасности, является целью работы многих компаний внутри Интернет-сообществ. Здесь главное отметить, пока большинство компаний по защите компьютерной информации, являются иностранными производителями и разработчиками. На первый взгляд высказывание это может показаться преувеличенным, но опасность вполне реальна.

Якунин А.С. в лице генерального директора «Воентелеком» утверждает, что «если задача обеспечения информационной безопасности при передаче по сетям и каналам связи может быть решена преимущественно с применением средств криптографической защиты информации отечественного производства, то обеспечение безопасности связи от разрушающих воздействий является проблемой, так как отсутствует собственная инфраструктура и поэтому «Воентелеком» вынужден заказывать необходимые услуги у коммерческих операторов связи, сети которых развернуты на импортном оборудовании».

Как видим, по мнению А.С. Якунина, «полноценно и гарантированно решать вопросы безопасности связи можно только тогда, когда в стране на сетях будет использоваться только российское телекоммуникационное оборудование, а еще лучше – будет создана единая выделенная сеть на его основе в интересах государственного управления». В настоящее время чипы, схемотехника, электронные компоненты, программное обеспечение и др., использующиеся в информационно-коммуникационной инфраструктуре в большинстве своём импортные с «чужой» начинкой. Учитывая это, даже после проведения специальной проверки и анализа всех вызывающих подозрение свойств и компонентов, нет полной уверенности в безопасности.

В России много успешных разработчиков по производству электроники, но им всё равно приходится взаимодействовать только с зарубежными чипвендорами. Поэтому для развития высокотехнологичной, конкурентноспособной продукции радиоэлектроники и программного обеспечения необходимо отечественному производителю взаимодействовать с отечественными разработчиками чипов внутри отрасли, что обезопасит, а также снизит зависимость России от иностранных производителей и разработчиков.

Так как проблемы кабербезопасности носят интегративный характер и не ограничиваются рамками инженерии, ситуация усугубляется еще повсеместным использованием мобильных устройств зарубежных производителей. Сегодня в Китае видят серьезную угрозу национальной безопасности в

платформе Android, так как правонарушители в большинстве случаев устремились к созданию и распространению зловредов для операционной системы Android. В 2022 году отмечен большой рост вредоносных программ для операционной системы Android, если за весь 2021 год было выявлено около 6000 новых вредоносных программ для всех мобильных платформ, то в некоторых месяцах 2022 года число обнаруженных зловредов превысило это число. В связи с чем, напрашивается вывод, что в настоящее время операционная система Android, является основной мишенью для создателей вирусов.

Руководителям ряда больших отечественных компаний на почту приходили письма с предложением отключить функцию автоматического обновления программного обеспечения и приложений на планшетах и смартфонах, так как в рамках возможных санкций может произойти блокировка их работы. Но, по мнению наших экспертов «такой механизм вряд ли обезопасит владельцев смартфонов ОС Android от дистанционного «блока», так как дополнительные ограничения, если они будут, могут затронуть разные сервисы: россияне лишатся почты, облачного хранилища, возможности слушать музыку, общаться через мессенджеры, и даже личных контактов, которые не были сохранены в памяти телефона. Но, скорей всего, добавляет программист, Apple и Google не пойдут на такой шаг» [5].

Из всего вышеперечисленного можно сделать вывод, что на сегодняшний день использование операционной системы Android, а также других мобильных платформ «чужого» производства является угрозой с точки зрения обеспечения информационной безопасности. Слабая конкуренция отечественных решений на международном рынке пока ставит перед необходимостью использовать аналоги импортного оборудования и программного обеспечения, что ещё раз подчеркивает необходимость комплексного подхода к организации производства электронных изделий и каналов сбыта инфокоммуникационных решений внутри страны [4].

Литература

1. Reliance spells end of road for ICT amateurs», May 07, 2013, The Australian.

2. Камбулатов Т.Г., Садыков С.И. Кибербезопасность в сети. В сборнике: Качество жизни населения и экология. Сборник статей Всероссийской научно-практической конференции. Пенза, 2021. С. 44-47.

3. Коротков С. О взаимосвязи куберпреступлений и международного гуманитарного права в контексте обеспечения международной безопасности. Международная жизнь. 22.12.2022. https://interaffairs.ru/news/show/38329.

4. Згоба Артём Игоревич, Маркелов Дмитрий Витальевич, Смирнов Павел Игоревич Кибербезопасность: угрозы, вызовы, решения // Вопросы

кибербезопасности. 2014. №5 (8). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya (дата обращения: 16.05.2023).

5. Код красный: как россияне будут жить без программного обеспечения. 18 марта 2022. https://dzen.ru/media/legalacademy/kod-krasnyi-kak-rossiiane-budut-jit-bez-programmnogo-obespecheniia-623489aaef6d237b562ed01b?utm_referer=www.google.com

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

Петрова Елена Владиленовна,
кандидат технических наук
старший преподаватель кафедры
автоматизированных информационных систем ОВД
Воронежского института МВД России

ОСОБЕННОСТИ УГРОЗ ЦИФРОВОГО ШПИОНАЖА ПРИ ВНЕДРЕНИИ СИСТЕМ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Представлены особенности угроз цифрового шпионажа, исходящих от систем искусственного интеллекта, анализирующих огромные массивы данных наносящих атаки потенциальным жертвам коммерческих компаний.

При выполнении задач сотрудниками Органов Внутренних Дел современные реалии диктуют условия для внедрения в процесс обработки потоков информации искусственного интеллекта (ИИ). Глубинное и машинное обучение меняет не только интернет, но и преступный мир.

Применение нейросетей и ботов для персонализации фишинг-атак корпоративного шпионажа и манипуляций через фейковый контент вызывают наибольшие опасения. Поэтому в системе ОВД в ближайшем будущем предстоит пересмотреть политики безопасности.

Одой из главных задач о допустимости применения ИИ для расследования преступлений является вопрос запрета использования ИИ для профилактики правонарушений. Эксперты опасаются, что злоупотребление функциями предиктивных систем приведет к тотальной слежке и утечке конфиденциальной информации в сеть.

В этой работе не затрагиваются сложные технические детали связанные с DDoS-атаками, использование одного ИИ для взлома другого и так далее. Разговор пойдет об ИИ-аналитиках (персонализации фишинга), ИИ-имитаторах (фейк-контенте) и как к новым угрозам готовиться уже сегодня.

Доказанно, что человек – субъективен и является самым слабым звеном корпоративной безопасности. Поэтому фишинг-атака со стороны киберпреступников главным образом направлена на то, чтобы заставить любыми путями нажать ссылку в фишинг-письме или в подставном окне регистрации ввести пароль. Число таких атак по данным Anti-Phishing Working Group за последний год побило всю историю наблюдения.

Искусственный интеллект создал мощное оружие в руках социальной инженерии в виде способности анализировать огромные массивы данных, как о потенциальной жертве коммерческой компании, так и физического

лица, занимающегося продажами на открытых интернет-сервисах, так сымитировав слог «приятеля» или официальное письмо, что на него кликнут без сомнений. Однозначно можно полагать, что «персонализация фишинга» ставится во главе ИИ-угроз.

За последний год обострилась проблема безопасности личных данных из-за эксплуатации доверия и невнимательности потребителя. Из-за не соблюдения простейших мер безопасности в открытый доступ попали терабайты клиентских баз и взломанных аккаунтов. По статистике, количество случаев хищения за третий квартал 2022 года снизилось более чем на 10% (230 тыс. эпизодов), однако общий размер ущерба вырос почти до 24% (почти 4 млрд рублей) [1].

Нейросеть создает контент который все сложнее отличить от настоящего, имитируя «живой» голос оператора фантастически имитируя человека. Поэтому дипфейки (подложные видео, созданные на основе других изображений) — можно поставить вторым в списке по масштабу ИИ-угроза.

Подобному контенту находится множество средств применения, основу которого составляет автоматизация вымогательских «call-центров» на основе роботов, способных имитировать голоса друзей. Применение в благих целях подобных чат-ботов происходит в основном в банковской сфере. Революционные подходы ИИ превращают товар «из коробки» в искусного бота с тонкими настройками киберпреступности.

Изменения затронули и политику. Агитационные чат-боты, распространявшие пропаганду, уже применялись на выборах в западных странах, но перспектива организованных вбросов из миллионов ботов, которых невозможно отключить из единой точки, выглядит пугающе, особенно на фоне распространения заведомо ложной информации о действиях российской армии А на фоне ответственности за фейки, введенной с 5 марта 2023 в законодательстве уголовная ответственность до 10 лет, может стать мощным инструментом конкурентной борьбы.

В современных условиях растет разнообразие преступных способов с применением беспилотных средств и их использования в атаках. К примеру, нейросети могут перехватить исходный код БПЛА и спланировать многоступенчатые теракты. Дроны, начиненные малым количеством взрывчатки – идеальное точечное оружие как для ликвидации субъекта, так и в масштабах автономных подлодок для переправки наркотиков. Начиная с 2018 года «дроновые скандалы» не сходят новостных полос. Военными экспертами констатированы варианты совершения атак «дронов-убийц» автономно.

В связи с вышеперечисленными угрозами безопасности (особенно безопасности российскому бизнесу, ослабленному санкциями) придется пересмотреть политики безопасности. Первоочередное внимание должно быть уделено инструктажу, постоянным тренировкам персонала и выстраиванию ИТ-защиты из спам-фильтров и таких программ, которые самостоятельно за-

секают опасное поведение (переход по подозрительным ссылкам, копирование служебных документов на сторонние носители и пр.), предупреждая службу безопасности.

Все большую актуальность принимают услуги пентестеров — агентства проверяющие компании на устойчивость к атакам, делая контрольные проверки офисов и представительств под видом стажеров своих корпоративных разведчиков. Ненавязчиво оставленная флэшка с вирусом, которую обязательно кто-то из сотрудников захочет проверить содержимое из любопытства, может нанести непоправимый урон компании.

Подводя черту вышесказанному можно смело утверждать, что ускорение обращения информации с внедрением ресурсов ИИ требует привлечения контркомпаний, способных в режиме реального времени отслеживать атаки и «вбросы» обеспечивая своевременный отклик на угрозы в сфере информационной безопасности.

Литература

https//www.cbr.ru/analytics/ib/review_3q_2022.

Петухов Андрей Юрьевич,
кандидат педагогических наук, преподаватель
Краснодарского высшего военного
училища им. генерала армии С.М. Штеменко

Картавцев Максим Сергеевич,
курсант Краснодарского высшего военного
училища им. генерала армии С.М. Штеменко

РАЗРАБОТКА АЛГОРИТМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА ТОНКОМ КЛИЕНТЕ С ИСПОЛЬЗОВАНИЕМ ОДНОРАЗОВЫХ ПАРОЛЕЙ

В современном мире, всё больше повышается спрос на использование систем терминального доступа на архитектуре аппаратных тонких клиентов. Однако, данное обстоятельство, также обуславливает необходимость обеспечения надлежащей защиты таких соединений от различных посягательств, особенно несанкционированного доступа.

Преимуществами использования данных систем, является то, что рабочая станция тонкого клиента не требует больших вычислительных возможностей. Для ее функционирования необходимы только устройства ввода-вывода информации и сетевая карта. Обработка и хранение данных происходит на сервере, что, в свою очередь, также повышает безопасность обрабатываемой информации[1].

Несмотря на наличие различных механизмов и средств защиты информации для пользовательских тонких клиентов, их корректность функционирования в значительной степени зависит от доверия к пользователям и к операционной системе, загружаемой по сети на рабочую станцию тонкого клиента.

Злоумышленник в случае физического проникновения в сетевую инфраструктуру, может подключиться к рабочей станции тонкого клиента, изменить параметры защиты системы и получить несанкционированный доступ к данным, циркулирующим на устройство[2]. Модель такого воздействия показана на рисунке 1. В связи с этим, необходим новый подход к повышению безопасности информации на тонких клиентах пользователей. Для этого, необходимо создать доверенную вычислительную среду, в которой

---

[1] Усовершенствование возможностей компьютерного парка кафедр факультета информационных технологий ВУЗа за счет использования терминальной архитектуры и технологии «Тонкий клиент». Колесников А.В., Маслова М.А. [Текст] // Перспективы развития информационных технологий. – 2015. – № 23. – С.126 -132.

[2] Модель доверенной сетевой загрузки «Тонкого клиента» с нейтрализацией «Внутреннего нарушителя». Тищенко Е.Н., Буцик К.А., Деревяшко В.В. [Текст] // Известия Южного федерального университета. Технические науки. – 2015. – Т.5. – С. 37-47.

будет достоверно известно, что все элементы сетевого взаимодействия не подвержены изменениям или воздействиям злоумышленника.

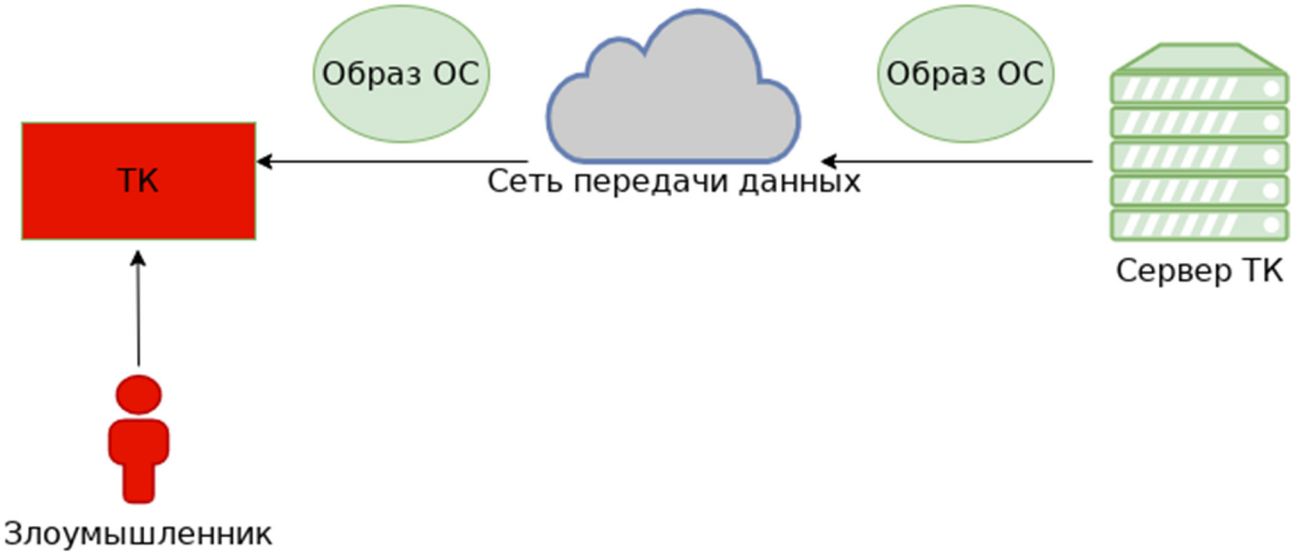


Рис. 1. Воздействие злоумышленника на тонкий клиент
сетевой инфраструктуры терминального доступа

В настоящее время основной проблемой является то, что существующие методы создания доверенной вычислительной среды для систем терминального доступа не всегда обеспечивают надлежащую безопасность, в связи с особенностями построения архитектуры тонких клиентов[1].

Для решения данной проблемы предлагается алгоритм аутентификации пользователя и рабочей станции тонкого клиента при помощи идентификатора доступа (токена), реализованного в виде защищенного usb-носителя. Общий принцип работы данного алгоритма состоит из использования пароля, который применяется только один раз при подключении, а после успешной аутентификации, генерируется новый и записывается на защищенный usb-носитель. Данный алгоритм отличается от существующих, тем, что за счет использования одноразовых паролей, исключается возможность их компрометации и повышается надежность.

Для реализации данного алгоритма необходимо понимать, что пользователь может подключать защищенный usb-носитель к любой рабочей станции сети терминального доступа и, для успешной аутентификации, пароли на защищенном usb-носителе и рабочих станциях должны совпадать. Для

---

[1] Алгоритм аутентификации участников информационного взаимодействия при удаленной загрузке операционной системы на тонкий клиент. Гатчин Ю.А., Теплоухова О.А. [Текст] // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т.16. №3. – С. 497-505.

этого на тонких клиентах должен быть одинаковый алгоритм генерации паролей, использующий один закрытый ключ. В процессе генерации паролей используется хэш-функция или алгоритм симметричного шифрования.

Перед началом работы алгоритма, администратором информационной безопасности производится первичная инициализация токена, в процессе которой токен получает от рабочей станции случайное число X, и его эталонный ответ Нэ-I(X) – зашифрованное значение X на закрытом ключе тонкого клиента I. Также записывается эталонное значение пароля пользователя Ртк.

Реализация алгоритма представлена на рисунке 2:

1. При запросе аутентификации пользователь получает на мониторе форму авторизации, которая предлагает вставить защищенный usb-носитель, и выполняет данное действие.

2. Рабочая станция запрашивает случайное число X, и токен передает его.

3. Тонкий клиент зашифровывает X, на закрытом ключе I, и передает зашифрованное значение Нтк-I(X) обратно защищенному usb-носителю.

4. Защищенный usb-носитель сравнивает полученное Нтк-I(X) с эталонным Нэ-I(X), в случае успеха, передает на ТК, подтверждение о прохождении аутентификации рабочей станцией.

5. Защищенный usb-носитель делает запрос у рабочей станции на пароль P, а рабочая станция запрашивает его у пользователя.

6. Пользователь производит ввод пароля Ртк на рабочей станции.

7. Рабочая станция предоставляет Ртк введенный пользователем на защищенный usb-носитель для сравнения.

8. Защищенный usb-носитель сравнивает Хтк с эталонным значением Хэ и возвращает результат на рабочую станцию. В случае положительного результата алгоритм завершается – пользователь аутентифицирован. В противном случае пользователь повторно вводит пароль ограниченное количество раз.

После успешного выполнения алгоритма аутентификации рабочая станция генерирует новое случайное число X’, зашифровывает его на ключе I, и передает на токен X’, и Нэ’-I(X). Данные значения записываются на токен и используются при следующем подключении. Это позволяет обеспечить удобство использования системы, так как пользователю не нужно каждый раз вводить новый пароль. Однако, такой подход не лишен недостатков. В частности, все рабочие станции должны применять общий ключ I для генерации паролей, что означает, что компрометация этого ключа может привести к несанкционированному доступу ко всем защищенным usb-носителям, инициализированным с использованием этого ключа. Следовательно, безопасность всей системы в целом будет зависеть от защищенности этого ключа, что является основным недостатком данного алгоритма

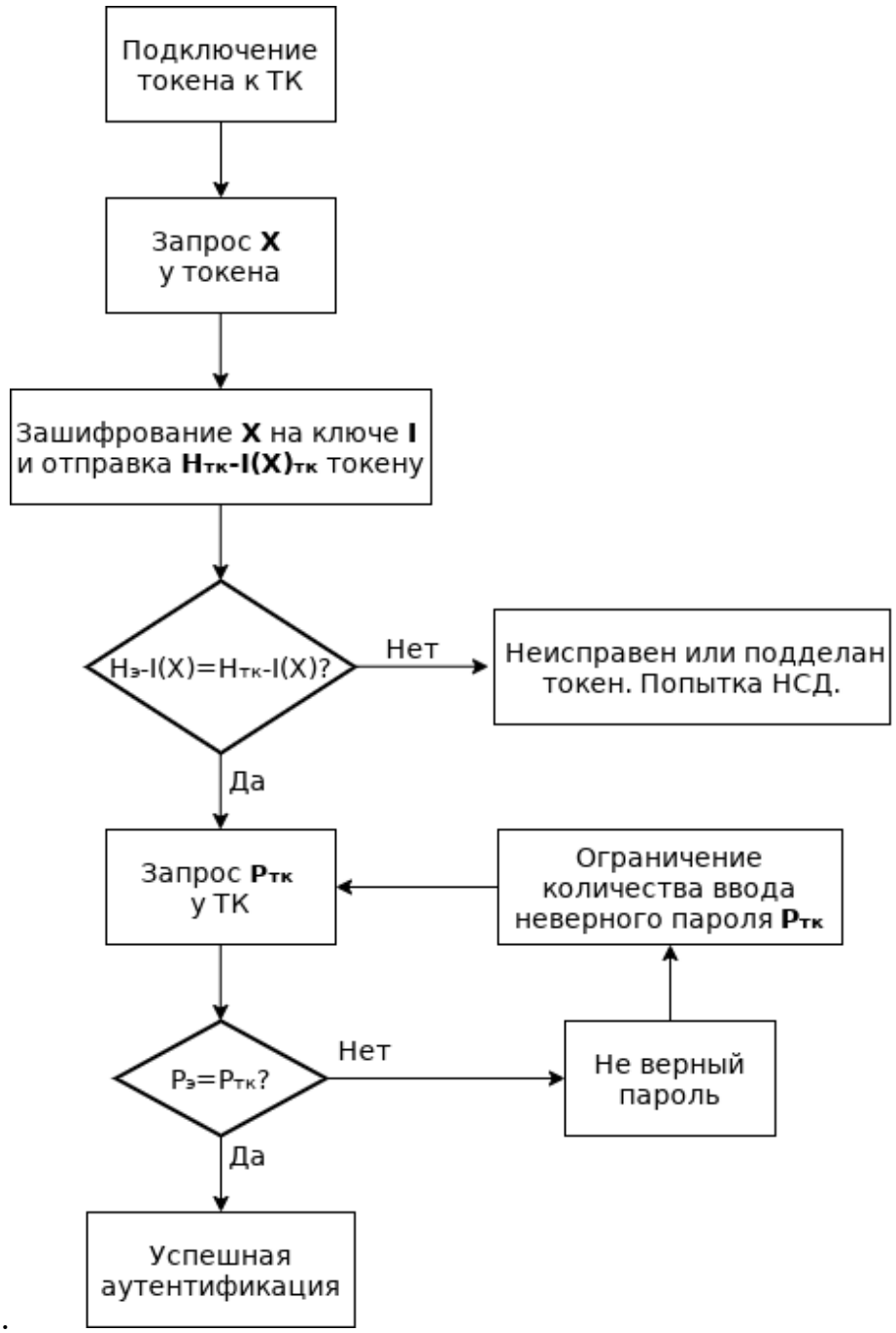


Рис. 2. Алгоритм аутентификации пользователя и рабочей станции тонкого клиента организации при помощи идентификатора доступа (защищенного usb-носителя).

Полученный алгоритм аутентификации пользователя и рабочей станции тонкого клиента, реализуемый при помощи идентификатора доступа (токена), реализованного в виде защищенного usb-носителя, достаточно прост и не ограничивает выбор архитектурной составляющей и операционной системы. Его применение возможно при разработке тонких клиентов в защищенном исполнении (совместно с защищенным usb-носителем).

Литература

1. Алгоритм аутентификации участников информационного взаимодействия при удаленной загрузке операционной системы на тонкий клиент. Гатчин Ю.А., Теплоухова О.А. [Текст] // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т.16. №3. – С. 497-505.

2. Модель доверенной сетевой загрузки «Тонкого клиента» с нейтрализацией «Внутреннего нарушителя». Тищенко Е.Н., Буцик К.А., Деревяшко В.В. [Текст] // Известия Южного федерального университета. Технические науки. – 2015. – Т.5. – С. 37-47.

3. Усовершенствование возможностей компьютерного парка кафедр факультета информационных технологий ВУЗа за счет использования терминальной архитектуры и технологии «Тонкий клиент». Колесников А.В., Маслова М.А. [Текст] // Перспективы развития информационных технологий. – 2015. – № 23. – С.126 -132.

Петухов Андрей Юрьевич,
кандидат педагогических наук, преподаватель
Краснодарского высшего военного
училища им. генерала армии С.М. Штеменко

Ковешников Михаил Андреевич,
курсант Краснодарского высшего
военного училища им. генерала армии С.М. Штеменко

РАЗРАБОТКА АЛГОРИТМА СЕТЕВОГО ЭКРАНИРОВАНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Современный мир трактует условия, в которых необходимо повсеместно использовать информационные ресурсы, отсюда появляется необходимость в постоянном усовершенствовании средств защиты всех элементов среды взаимодействия, это влечет усложнение средств информационной безопасности и, как следствие, увеличение затрат на их администрирование. Работа со средой облачных вычислений предполагает использование средств защиты (межсетевые экраны) на протяжении всего пути передачи пакета от объекта к субъекту и обратно. Поэтому, появляется необходимость разработки оптимального алгоритма работы сетевого экрана, посредством использования политики доступа с помощью правил фильтрации трафика.

Для решения этой задачи, перспективным направлением является оптимизация работы используемых межсетевых экранов, защищающих среду облачных вычислений. В рамках этой задачи необходимо формализовать требования взаимодействия в среде облачных вычислений, оптимизировать их, путем включения в работу алгоритма правил фильтрации трафика, сетевых соединений. Также необходимо обозначить работу сервиса управления межсетевыми экранами который будет осуществлять предварительную фильтрацию пакетов и сетевых соединений, дальнейшее распределение на виртуальные машины осуществляющее их обработку.

Целью исследования, является разработка алгоритма, позволяющего оптимизировать эффективность сетевого экранирования в среде облачных вычислений.

В области информационной защиты компьютерных систем правильное построение и настройка политики безопасности гарантирует создание и поддержание состояния защищенности в условиях воздействия внешних угроз[1].

Любые процессы в компьютерной системе выполняются в условиях дискретного времени. Представим отдельно взятый временной интервал, за

---

[1] Модели безопасности компьютерных систем. Куликов С.С.// учеб. пособие. - Воронежский государственный технический университет. - 2015. - №1. - С.7-11.

это время в компьютерной системе функционировало бесчисленное множество субъектов и объектов системы, выполняющих свою определенную роль. Поэтому, под субъектом в данном случае будет пониматься выполняющий процесс (активный), а под объектом системы мы понимаем изменяемую группу ресурсов (пассивный), также объект в данном случае может выступать в роли жертвы воздействия негативного субъекта, получившего возможность совершать действия в отношении объекта компьютерной системы. Схема взаимодействия субъекта и объекта среды, защищенная монитором безопасности представлена на рис. 1.

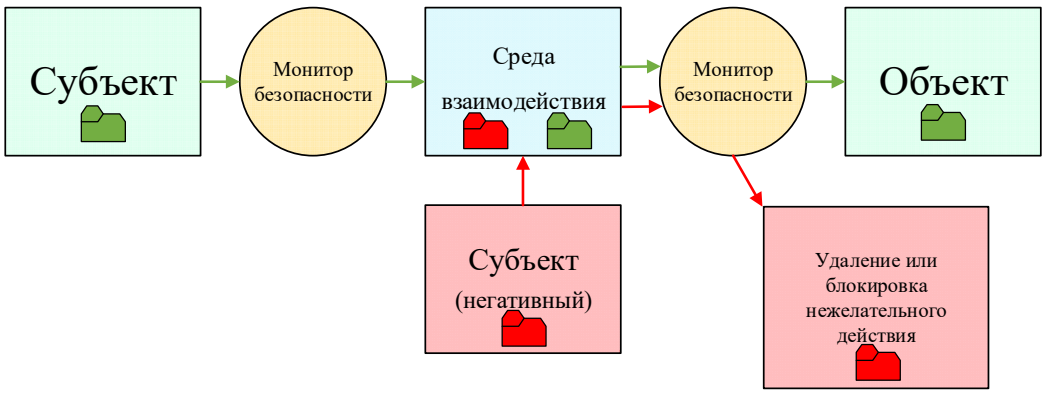


Рис. 1. Схема взаимодействия субъекта и объекта компьютерной системы

На рисунке, представлена схема взаимодействия субъекта и объекта компьютерной системы, основным элементом данной системы, обеспечивающим безопасное взаимодействие активной и пассивной сущности, а также управление доступом и контроль распределения данных передаваемых в среде будет являться «Монитор безопасности».

Субъектом установленной политики безопасности в данной среде будет являться монитор безопасности, своими настройками способствуя формированию и поддержанию работы выбранной модели безопасности. Компьютерная система безопасна если, и только если активные сущности (субъекты) не имеют права обходить определенную ранее политику безопасности среды[1].

Для описания представленного информационного взаимодействия, появилась необходимость разработать модель описывающей работу политики разграничения доступа с учетом постоянно изменяющихся характеристик среды. Создание модели обуславливается необходимостью практического представления процессов протекающих в среде облачных вычислений, а именно взаимодействия между субъектом и объектом в среде с постоянно

---

[1] Информационная безопасность автоматизированных систем. Солодянников А.В. // учеб. пособие. - Санкт-петербургский государственный экономический университет. - 2020. - №1. - С.19-26.

изменяющимися характеристиками. Описание модели дает возможность разработать необходимые правила фильтрации, которые позволяют существенно понизить нагрузку на межсетевые экраны и осуществляют предварительную фильтрацию поступающих пакетов.

Для создания правил безопасного взаимодействия в среде облачных вычислений наиболее подходящей моделью будет являться ролевая модель разграничения доступа[1]. В процессе формирования данной модели разграничения доступа появляется необходимость ввести еще один активный процесс – роль.

Рассматриваемый метод с зоной предварительной фильтрации для мониторов безопасности упрощает процесс работы сформированной политики разграничения доступа, представленной для формирования и работы большого числа виртуальных машин, запущенных на базе единого «облака»[2]. Полномочия для каждого субъекта, имеющего роль, сформировываются на основании закрепленных за ним правил фильтрации, созданных на основании передаваемых им данных. Для представленной системы автором выбрана наиболее перспективная политика «все что не разрешено, запрещено». Вся информации о роли необходимая для формирования взаимодействия находится в сервисе управления межсетевыми экранами, представленной на рис. 2.

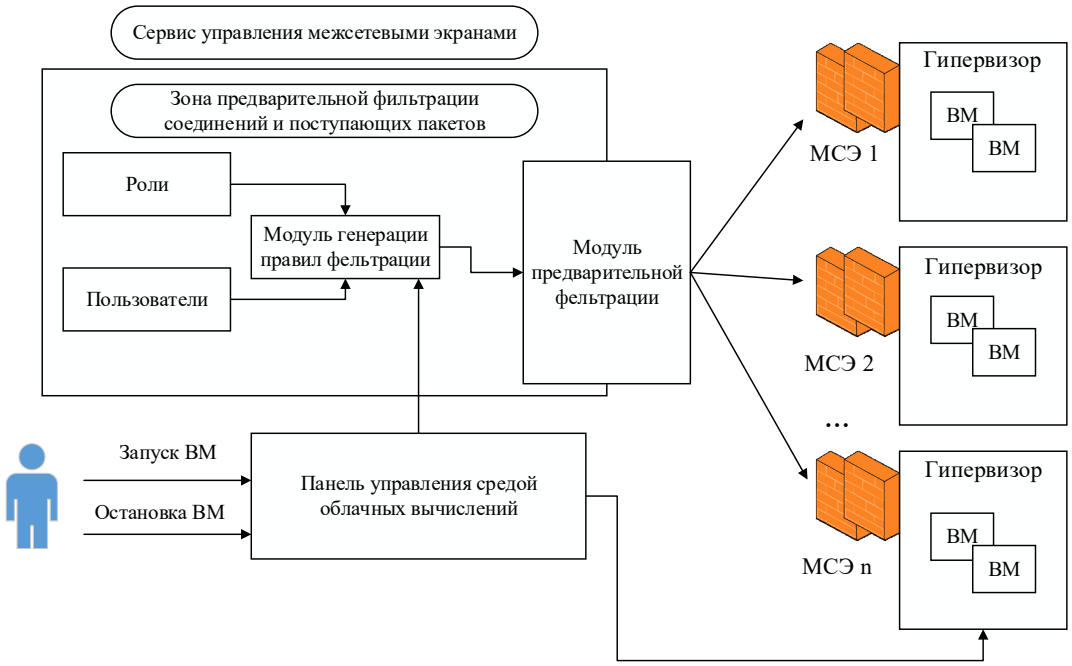


Рис. 2. Схема управления межсетевыми экранами для метода информационного взаимодействия

---

[1] Модели безопасности компьютерных систем. Богульская Н.А., Кучеров М.М.// учеб. пособие. - Сибирский федеральный университет. - 2019. - №1. - С.113-118.

[2] Система защиты информационного взаимодействия в среде облачных вычислений. Лукашин А.А.// диссертация. - Санкт-петербургский государственный политехнический университет. - 2012. - №1. - С. 57-60

На основании, представленной схемы, нами разработан алгоритм, реализующий механизм предварительной фильтрации. Поступавший пакет(новый) направляется в поток для осуществления первичной обработки, производится анализ протоколов и виртуального соединения, по которому был передан данный пакет. При первичной обработке соединению и пакету назначаются отдельные обработчики. Если в процессе обработки выясняется, что соединение и пакет являются безопасными, то происходит их выполнение, а необходимая информация сохраняется и про повторное подключение обработка назначаться не будет. Алгоритм модуля предварительной фильтрации представлен на рис. 3.

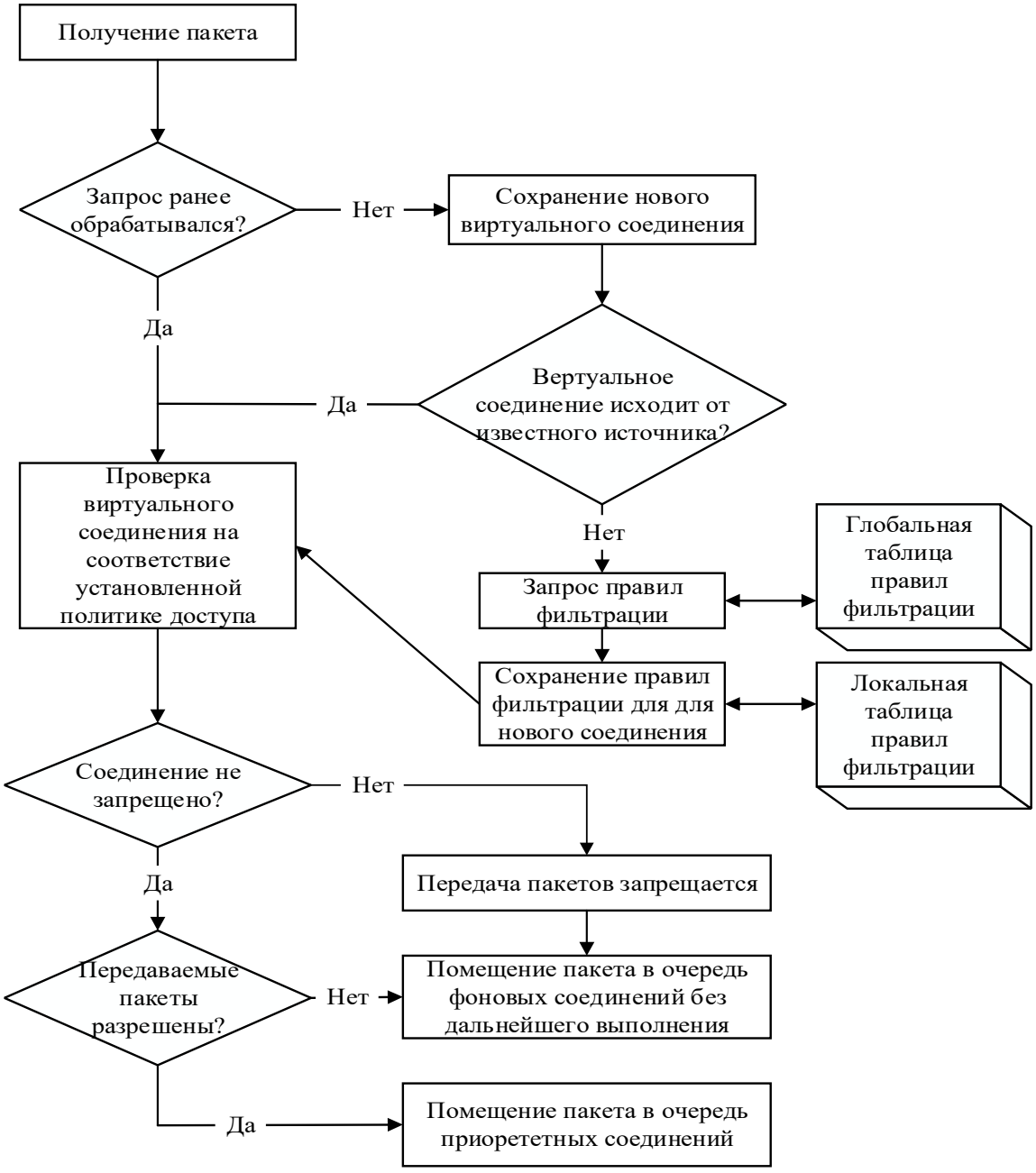


Рис. 3. Алгоритм фильтрации виртуального соединения
и пакетов информационного взаимодействия

Данный алгоритм выполняется в отдельном потоке, после завершения, в зависимости от исхода происходит дальнейшее распределение пакетов в одну из сформированных очередей:

– очередь разрешенных к выполнению пакетов;

– очередь запрещенных к выполнению пакетов.

Для упрощения функции контроля, с целью оптимизации процесса вся информация о разрешённых подключениях будет храниться в памяти, взаимодействовать с которой сможет только обработчик. Необходимые для работы обработчика правила фильтрации будут загружаться непосредственно из памяти.

В данной работе решалась задача разработка алгоритма позволяющего оптимизировать эффективность сетевого экранирования в среде облачных вычислений. В ходе решения данной задачи разработан алгоритм, позволяющий оптимизировать работу монитора безопасности (межсетевого экрана) выполняющего защиту информационного взаимодействия в среде облачных вычислений.

Литература

1. Информационная безопасность автоматизированных систем. Солодянников А.В.// учеб. пособие. – Санкт-петербургский государственный экономический университет. – 2020. – №1. – С.19-26.

2. Модели безопасности компьютерных систем. Богульская Н.А., Кучеров М.М.// учеб. пособие. – Сибирский федеральный университет. – 2019. – № 1. – С.113-118.

3. Модели безопасности компьютерных систем. Куликов С.С.// учеб. пособие. – Воронежский государственный технический университет. – 2015. – № 1. – С.7-11.

4. Система защиты информационного взаимодействия в среде облачных вычислений. Лукашин А.А.// диссертация. – Санкт-петербургский государственный политехнический университет. – 2012. – № 1. – С. 57–60.

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

ОСОБЕННОСТИ ПОИСКА ЭКСТРЕМИСТСКОЙ ИНФОРМАЦИИ В ОТКРЫТЫХ ИСТОЧНИКАХ СЕТИ ИНТЕРНЕТ

В настоящее время, с развитием информационных технологий у человека появилась возможность получать огромное количество информации, зачастую не разбираясь в источниках и авторах данной информации. Это создает благоприятные условия для развития международного экстремизма и терроризма.

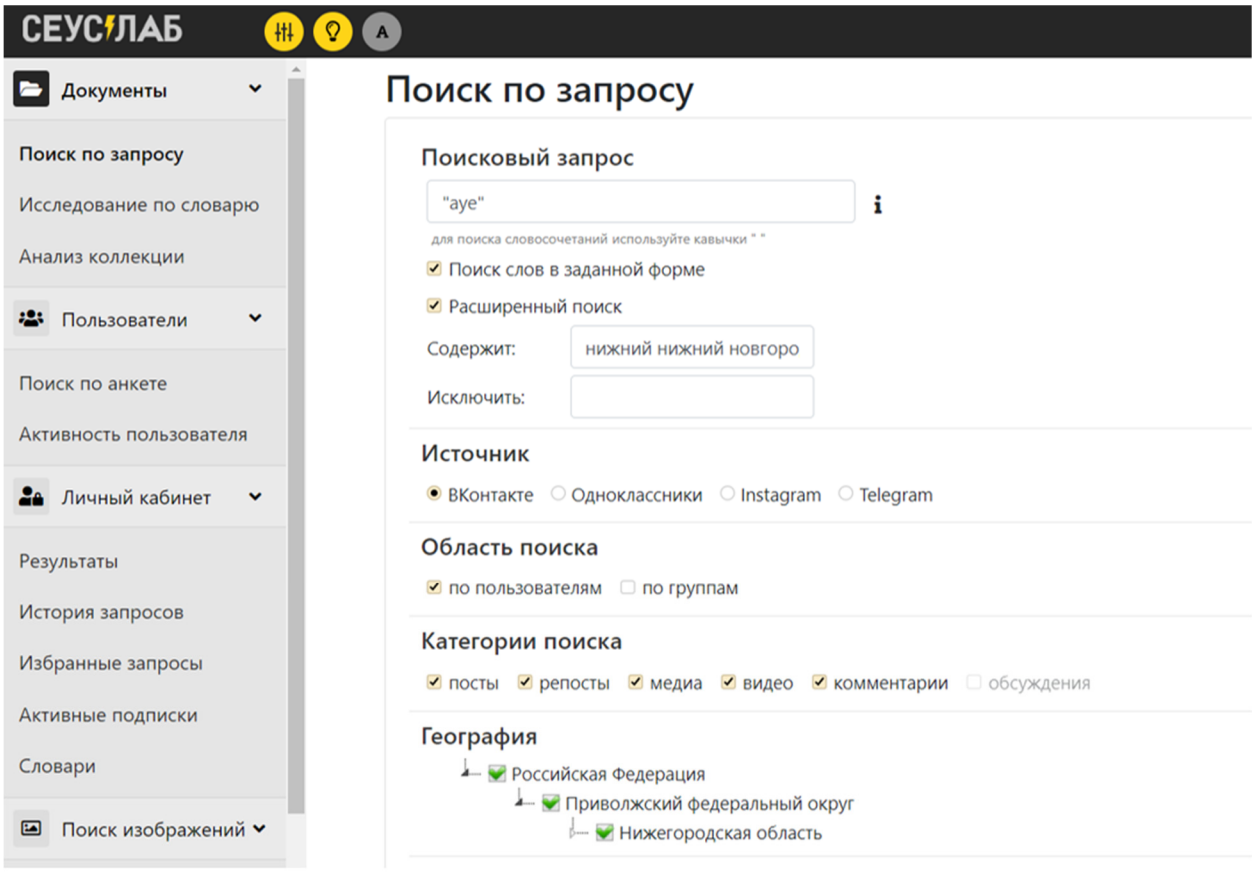
Актуальность данной тематики подтверждается статистикой. В 2022 году зарегистрировано свыше полутора тысяч преступлений экстремистской направленности, большинство из которых совершается при помощи информационно-телекоммуникационной сети «интернет».

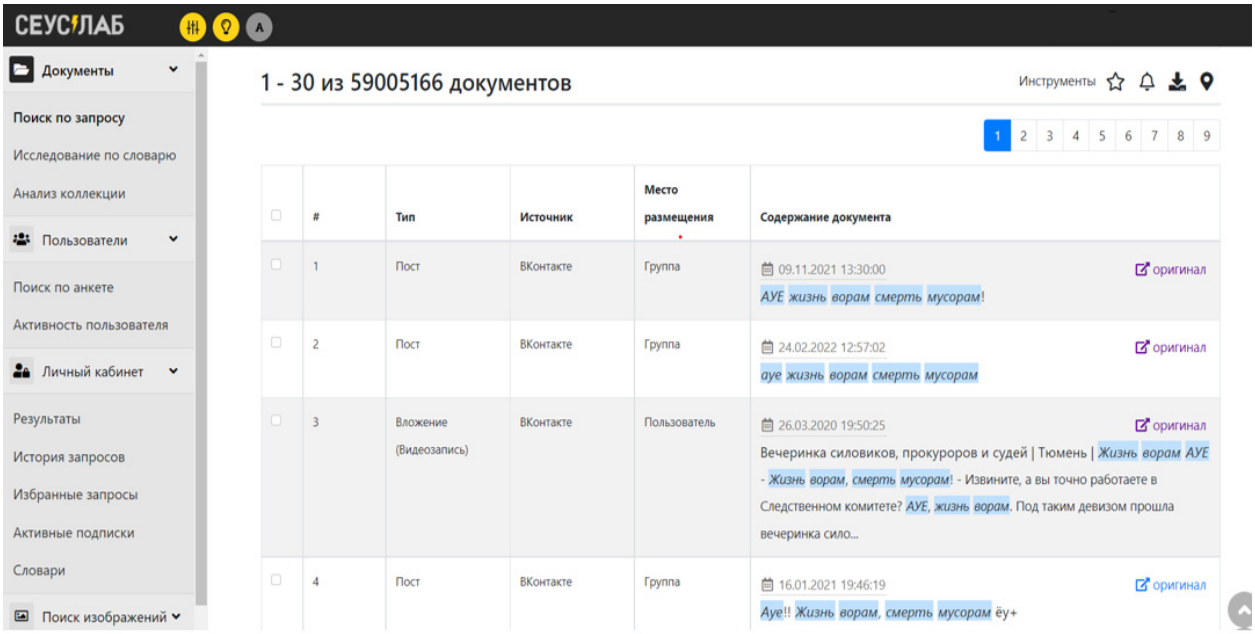
Экстремизм или экстремистская деятельность – призыв людей к совершению каких-либо действий, направленных против государства или определенных слоёв населения, социальных групп, а терроризм или террористическая деятельность – это преступление против государства или определенных слоев населения, социальных групп, нарушение общественной безопасности, которое выражается в посягательстве на жизнь и здоровье, природную среду, экологию, объекты инфраструктуры и тому подобное для устрашения населения или дестабилизации деятельности государства. Таким образом, мы видим, что экстремизм и терроризм может проявляться и в интернете посредствам пропаганды, с помощью которой террористы влияют на мировоззрение людей, внушая им свои взгляды или настраивают население против власти, тем самым дестабилизируя государство. Так же посредствам интернета, социальных сетей или иных сайтов террористы вербуют людей.

Людей для вербовки террористические организации ищут, как правило в социальных сетях, публикуя на своих страницах материалы экстремистской или террористической направленности, либо в группах, каналах, комментариях, личной переписке и т.д.

Таким образом, мы видим, что для осуществления своей деятельности террористическим и экстремистским организациям необходимо публиковать материалы соответствующей направленности в открытых источниках, где их уже может найти сотрудник органов внутренних дел или специальное программное обеспечение. Программа «СЕУСЛАБ», используемая специальными подразделениями органов внутренних дел обеспечивает поиск подобной информации и выявляет данные преступления в таких социальных сетях и мессенджерах как: «В контакте», «Одноклассники», «Instagram» и «Telegram».

В использовании программа проста, интерфейс интуитивно понятный, после заполнения всех необходимый полей сотрудник осуществляет поиск и получает результаты.





Далее сотрудник специального подразделения далее сотрудник оценивает на сколько данные материалы можно считать экстремистскими или террористическими и принимает процессуальные решения.

Таким образом мы видим, что в настоящее время увеличивается количество экстремистских преступлений в «интернете», а для их поиска и пресечения у сотрудников органов внутренних дел присутствует необходимое программное обеспечение.

Погудин Иван Николаевич,
ведущий научный сотрудник
отдела разработки и внедрения криминалистической техники
центра сопровождения НИОКР в области
информационных технологий ФКУ НПО «СТиС» МВД России,
кандидат технических наук, доцент

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ СОЗДАНИЯ УНИВЕРСАЛЬНОЙ МАСШТАБИРУЕМОЙ ЛАБОРАТОРИИ ДЛЯ ПРОИЗВОДСТВА КОМПЬЮТЕРНЫХ ЭКСПЕРТИЗ

Аннотация:
Исследована возможность создания универсальной масштабируемой лаборатории для производства компьютерных экспертиз, определены ее функции, задачи и возможная структура построения.

Ключевые слова и словосочетания: компьютерная экспертиза, аппаратно-программный комплекс, масштабируемая лаборатория.

Одним из приоритетных направлений деятельности МВД России в настоящее время в условиях активного развития цифровых технологий и их широкого внедрения в жизнь современного общества является противодействие киберпреступности.

Злоумышленники овладели принципиально новыми высокотехнологичными методами совершения преступлений, которые создают угрозы для многочисленных сфер общественной жизни.

В последние годы наблюдается тенденция увеличения доли зарегистрированных киберпреступлений. Значительный рост киберпреступлений в сфере посягательства на частную и государственную собственность, незаконным оборотом наркотических средств и психотропных веществ, мошенничеством в финансово-кредитной сфере произошел в период 2020–2021 гг. Большинство киберпреступлений совершается с использованием сети интернет или при помощи мобильной связи. За последние 5 лет число киберпреступлений в России выросло в 11 раз, их удельный вес в структуре преступности вырос с 1.8 % до 25 %.[1]. В 2020 году число преступлений с использованием информационно-телекоммуникационных технологий (ИТТ) выросло на 73,4 %, в т.ч. с использованием сети «Интернет» – на 91 %, при помощи средств мобильной связи – на 88,3 %.[2]

---

[1] Число киберпреступлений в России выросло в 11 за пять лет. [Электронный ресурс]. URL: http//tass.ru/obschestvo/10616343 (дата обращения 06.03.2023).

[2] Статистика. Состояние преступности в России за январь-декабрь 2020 г. [Электронный ресурс]. URL: hhtps:мвд.рф/reports/2 (дата обращения 06.03.2023).

В связи с этим борьба с киберпреступностью остается первостепенной задачей правоохранительных органов. Директивой МВД России[1] противодействие преступлениям в сфере ИТТ определено в качестве одного из приоритетных направлений деятельности МВД России, поэтому в органах внутренних дел возрастает потребность в проведении специальных компьютерных видов судебных экспертиз.

В настоящее время для производства компьютерных экспертиз применяются в основном унитарные аппаратно-программные комплексы (АПК), построенные по принципу «все в одном» (например АПК «Композиция»). Их архитектурное решение построено на использовании одной рабочей станции, в состав которой входят все необходимые на момент разработки интерфейсы для подключения исследуемых объектов, а также программное обеспечение, позволяющее решать большинство задач, относящихся к разряду классических для современной судебной компьютерной экспертизы.

Такое решение доказало свою универсальность и на данный момент повсеместно применяется в экспертных подразделениях системы МВД России и других силовых ведомств. Однако в составе существующих аналогов имеются устаревшие комплектующие, снятые с производства; отсутствует возможность исследования вновь появившихся объектов; не предусмотрены современные методы исследований, как новых, так и традиционных объектов; отсутствует возможность автоматизации исследований; не реализована возможность динамического перераспределения вычислительных ресурсов, объемов хранения информации и доступа к программному обеспечению криминалистического назначения. Кроме этого проведение компьютерных экспертиз сегодня можно считать эффективным в отношении лабораторий, в которых работает один или два эксперта. При использовании унитарных стендов в более крупных подразделениях начинают проявляться такие недостатки как:

– неэффективность использования вычислительных мощностей;

– постоянный недостаток объемов хранилищ информации в результате их нерационального распределения и использования;

– избыточность лицензионной нагрузки программного обеспечения;

– простой оборудования (в нерабочее время, по окончании процесса исследования, технологического процесса);

– высокие потери служебного времени эксперта на ожидание завершения технологических операций при проведении длительных исследовательских процессов;

– недостаточный контроль над исследуемыми объектами в момент временного отсутствия эксперта на рабочем месте.

Состоящее на снабжении органов внутренних дел оборудование не позволяет решать такие задачи как:

---

[1] Директива МВД России от 3 ноября 2021 г. № 1дсп.

– исследование следовой картины преступлений, совершенных с использованием специально написанного либо приспособленного программного обеспечения (ПО), в том числе ПО, имеющего недекларируемые возможности;

– построение «цифрового полигона» для исследования следовой картины преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий;

– вопросы, связанные с обработкой большого массива данных, полученных при исследовании группы объектов в рамках проведения экспертного исследования.

В связи с этим возникает необходимость повышения уровня обеспечения экспертно-криминалистического сопровождения деятельности подразделений системы МВД России посредством разработки и создания АПК для криминалистического исследования всех актуальных на настоящее время объектов носителей компьютерной информации, мобильных устройств, программного обеспечения, массивов данных и других объектов компьютерной экспертизы.

АПК должен обеспечивать решение следующих задач:

1. Исследование накопителей на жестких магнитных дисках (НЖМД);

2. Обеспечение доступа к информации, находящейся на неисправных НЖМД;

3. Исследование накопителей на картах памяти, USB Flash и SSD;

4. Восстановление поврежденной и удаленной информации, находящейся на компьютерных носителях информации;

5. Поиск пользовательской информации, находящейся на исследуемом носителе;

6. Автоматизированное исследование информационных объектов операционных систем (ОС) семейства Windows;

7. Проведение экспертизы карт с магнитной полосой и смарт-карт;

8. Проведение экспертизы сотовых телефонов;

9. Проведение анализа информации, содержащейся в служебных файлах ОС Linux;

10. Восстановление работоспособности АПК.

Исходя из перечня решаемых задач, АПК должен состоять из следующих компонентов:

1. Управляющий сервер, на котором развернуто:

– системное ПО (с открытым исходным кодом);

– ПО для эмуляции аппаратного обеспечения различных платформ с открытым исходным кодом;

– прикладное ПО для управления мощностями и задачами ресурсных серверов.

2. Два ресурсных сервера на базе ОС Linux и Windows, на каждом из которых развернуто системное ПО с открытым исходным кодом и программным управлением, обеспечивающим связь и передачу управления

управляющему серверу с возможностью установки дополнительного серверного ПО.

3. Рабочая станция администрирования, для использования в режиме Клиент-Сервер в целях дистанционного контроля за сетевой активностью и процессами на управляющем сервере.

4. Три клиентские стендовые ПЭВМ, для использования в качестве терминалов, которые можно использовать как в режиме Клиент-Сервер, так и в режиме локальной рабочей станции. Кроме этого, на клиентских стендовых ПЭВМ должна быть реализована поддержка развертывания образа исследуемого объекта для дистанционного контроля за сетевой активностью и процессами.

5. Коммутационное и сетевое оборудование (маршрутизатор, коммутатор, модем, сетевые кабели и др.), обеспечивающее возможность построения различных конфигураций локальной сети.

6. Ноутбук (для осмотра места происшествия).

7. АПК для снятия образов с мобильных устройств и проведения их логического анализа.

8. Набор НЖМД и USB-накопителей для создания копий носителей информации, образов оперативной памяти и пр.

9. Общее программное обеспечение.

10. Специальное программное обеспечение.

Общее системное и прикладное ПО должно состоять из:

1. Серверные ОС на базе Linux и Windows;

2. ОС рабочих станций на базе Windows;

3. Microsoft Office;

4. Средства резервного копирования информации;

5. Антивирусные продукты и др.

Специальное ПО должно выполнять следующие функции:

1. Поиска и анализа следовой картины (ПО криминалистического назначения);

2. Организации резервного копирования («быстрых бэкапов») и восстановления ОС;

3. Динамического программного анализатора;

4. Межсетевого экрана (брандмауэр), для контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами;

5. Хэширования данных;

6. Исследования кода программы (редакторы файлов, анализаторы исполняемых файлов – детекторы EXE компиляторов и упаковщиков, средства для контроля за работой различных программ и др.);

7. Анализа и модификации откомпилированных исполняемых файлов и библиотек («отладчики» для разных ОС);

8. Мониторинга и анализа скрытых функций (инструменты, способные показать информацию, которую разработчики сделали недоступной для пользователя программы);

9. Декомпиляции исполняемых файлов и инсталляционных пакетов;

10. Исследования и поддержки криптоалгоритмов;

11. Распаковки запакованных и защищенных исполняемых файлов;

12. Подбора паролей;

13. Исследования программ мобильных устройств.

В зависимости от сложности выполняемых задач должна быть обеспечена возможность реализации следующих типовых конфигураций АПК:

1. Базовый вариант (Рис. 1) для малых лабораторий от трех клиентских рабочих станций экспертов (состав: 1 управляющий сервер, 2 ресурсных сервера, 1 рабочая станция администрирования и не менее 3 клиентских стендовых ПЭВМ).

Рис. 1 Базовый вариант АПК.

2. Максимальный вариант (Рис. 2). Для лабораторий до 52 клиентских рабочих станций экспертов (состав: 1 управляющий сервер, до 16 ресурсных серверов, не менее 1 рабочей станции администрирования и не менее 52 клиентских стендовых ПЭВМ).

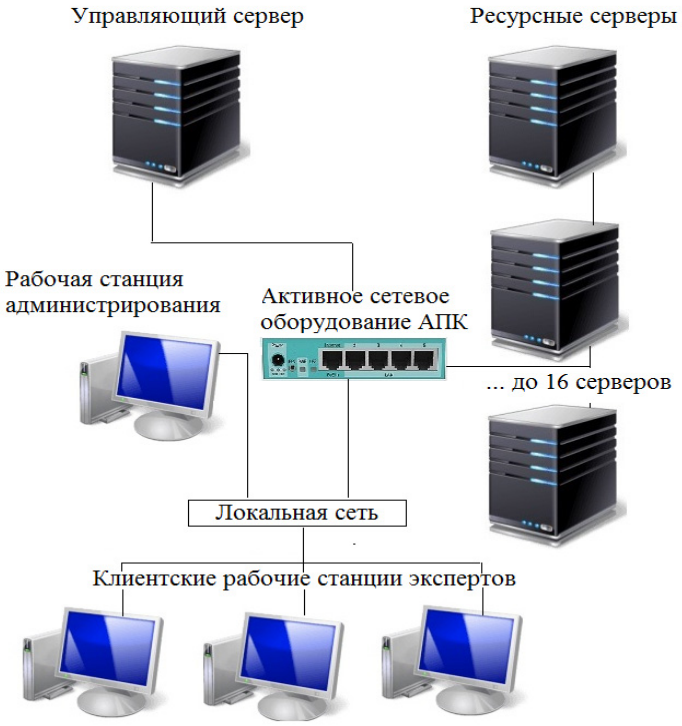


Рис. 2 Максимальный вариант АПК.

3. Произвольный вариант с любым количеством клиентских рабочих станций экспертов (от 3 до 52) и ресурсных серверов (от 2 до 16) (состав: 1 управляющий сервер, от 2 до 16 ресурсных серверов, не менее 1 рабочей станции администрирования и от 3 до 52 клиентских стендовых ПЭВМ).

Методом аппаратной виртуализации может быть обеспечено объединение ресурсных серверов в единый вычислительный массив, с целью образования общего пула вычислительных мощностей и ресурсов хранения компьютерной информации вариант (Рис. 3).

Рис. 3 Гипервизор.

Таким образом, создание универсальной масштабируемой лаборатории для производства компьютерных экспертиз (АПК) позволит обеспечить базовые экспертно-криминалистические подразделения системы МВД России современным стендовым оборудованием, помогающим проводить экспертное исследование всех актуальных на настоящее время объектов. За счет модульной конструкции и гибкой архитектуры предполагается создавать различные конфигурации АПК для одновременной работы от 3 до 52 экспертов и наращивать производительность и объемы хранения информации (от 2 до 16 ресурсных серверов) без замены основных компонентов АПК. Это позволит продлить жизненный цикл стендового оборудования и повысить эффективность его использования. Создание АПК также будет способствовать повышению функциональности и сокращению номенклатуры аппаратно-программных комплексов, принятых на снабжение органов внутренних дел Российской Федерации.

Разиньков Александр Сергеевич,
начальник отдела в г. Новороссийске ЦПЭ
ГУ МВД России по Краснодарскому краю

Куликов Кирилл Сергеевич,
оперуполномоченный отдела в г. Новороссийске
ЦПЭ ГУ МВД Росси по Краснодарскому краю

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДОКУМЕНТИРОВАНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ (НА ПРИМЕРЕ КРАСНОДАРСКОГО КРАЯ)

Массовое распространение информационно-телекоммуникационных технологий повлияло на нашу повседневную жизнь. Но помимо положительных аспектов, к примеру таких как доступ к различным познавательным ресурсам, обучение, хранение и передача различного рода информации, мы получаем и отрицательные аспекты. Безусловно примером негативного использования информационно-телекоммуникационных технологий является как раз и распространение негативного контента экстремисткой и террористической направленности. Теперь лицу, осуществляющему вербовку в запрещенную в Российской Федерации террористическую организацию или осуществляющего экстремистскую пропаганду, не нужно приезжать на территорию Российской Федерации или публично выступать, достаточно по средством сети Интернет разместить необходимые для достижения свой цели запрещенные материалы, которые в свою очередь могут быть замаскированы под развлекательный или образовательный контент. Связано это в первую очередь с развитием информационно-телекоммуникационных технологий и применением их злоумышленниками, в частности к примеру уход из открытых источников сети Интернет в «теневой» Интернет, посредством сети TOR, а также использование различных анонимных мессенджеров, таких как Telegram, Signal, Session и другие. А также передовое использование социальных сетей, в которых в большом количестве, посредством однодневных аккаунтов, созданных на неустановленные абонентские номера и электронные почты, происходит распространение экстремистских материалов.

Появление платежных систем на основе блокчейн технологий (криптовалют BTC, ETH, SOL, ADA и др.), также дает новые возможности в незаконном получении денег, отмывании денежных средств, полученных преступным путем, финансировании экстремистских и террористических организаций.

Приведём статистику преступлений экстремистской направленности в Краснодарском крае за 2023 год с использованием информационно-телекоммуникационных технологий:

За 4 месяца 2023 года в крае зарегистрировано 14 преступлений экстремистской направленности, из них:

1) 1 связано с созданием экстремистского сообщества и вовлечением в его деятельность (ч. 1. и ч.1.1 ст. 282.1 УК РФ),

2) 8 – с созданием экстремистской организации, вовлечением и участием в ее деятельности (ч. 1, ч. 1.1 и ч.2 ст. 282.2 УК РФ),

3) 3 преступления – с публичными призывами к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ) и

4) 2 преступления связаны с попыткой совершения убийства организованной группой лиц, в связи с осуществлением ими служебной деятельности, а также по мотивам идеологической, расовой, национальной ненависти в отношении лиц неславянской национальности, ведущих асоциальный образ жизни (п.п. «б», «ж», «з», «л» ч. 2 ст. 105 УК РФ).

За отчетный период 2023 года в крае зарегистрировано 17 преступлений террористического характера.

В ходе оперативно-розыскных мероприятий сотрудниками ЦПЭ ГУ МВД России по Краснодарскому краю выявлено 90 правонарушений экстремистской направленности.

В соответствии со ст.ст. 15.3, 15.3-1Федерального закона от 27.06.2006, № 149-ФЗ «Об информации, информационных технологиях и о защите информации», прокуратуры края для принятия мер прокурорского реагирования и ограничения доступа к Интернет-ресурсам направлено 100 материалов.

Основные проблемы, с которыми сталкиваются на практике сотрудники ЦПЭ ГУ МВД России по Краснодарскому краю:

1) Высокая динамика совершаемых преступлений;

2) Высокая латентность совершаемых преступлений;

3)Отсутствие на первоначальном этапе документирования идентифицированного субъекта преступления;

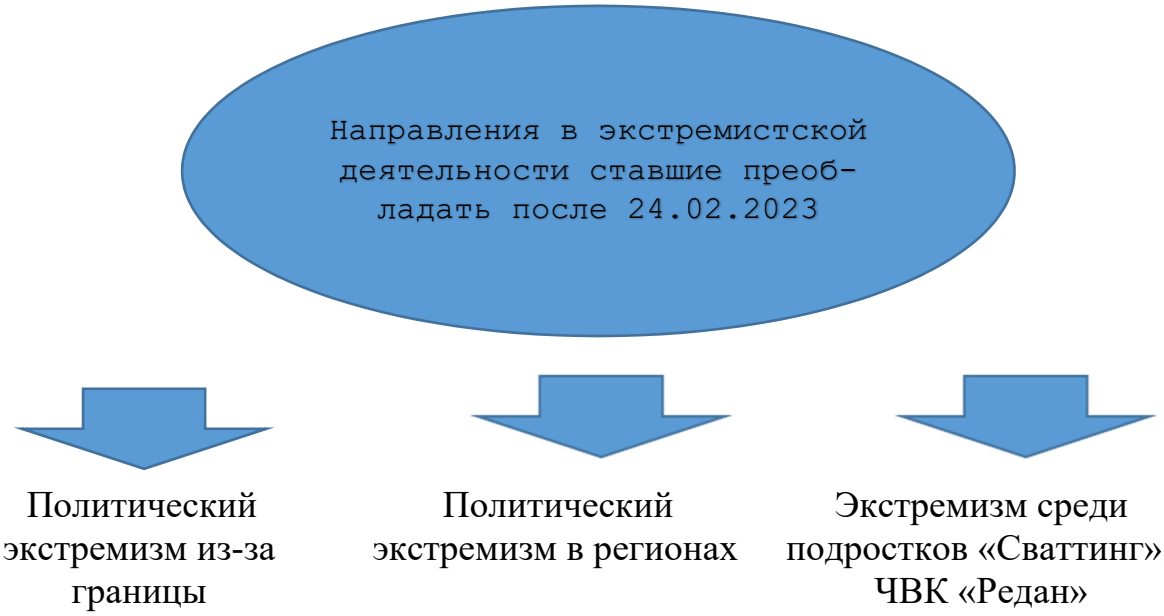
4)Сбор надлежащей доказательной базы на первоначальном этапе документирования;

5)Отсутствие технических возможностей контроля указанных систем со стороны правоохранительного органа.

Некоторые примеры использования информационных технологий сотрудниками ЦПЭ ГУ МВД России по Краснодарскому краю при документировании преступлений экстремистской направленности.

С началом СВО, и введению в уголовный кодекс новых статей идет тенденция на увеличение преступлений, совершаемых с использованием информационно-телекоммуникационных сетей в сфере экстремистской деятельности.

Сегодня актуально поговорить о преступлениях формирующих свою структуру исходя из складывающейся обстановки, непосредственно хотелось бы затронуть так называемые два лагеря, состоящие из лиц, поддерживающих СВО и лиц негативно к ней относящихся, для этого в своей статье мы выделим три наиболее важных направления:



Рассмотрим данные виды экстремизма на некоторых конкретных примерах в оперативно-служебной деятельности за 2023 год Центра по противодействию экстремизму ГУ МВД России по Краснодарскому краю.

Под политическим экстремизмом из-за границы мы будем рассматривать граждан России покинувших территорию России и ведущих свою противоправную протестную деятельность за пределами Российской Федерации.

Политический экстремизм из-за границы: примером № 1 может служить Николай (ФИО с целью неразглашения сведений не раскрываются), который покинул территорию России и в настоящее время находится в г. Марсель (Франция).

Он активно ведет свою протестную деятельность в сети Интернет в мессенджере «Телеграмм», где в тематических протестных группах:

–призывает граждан к борьбе против действующей власти Российской Федерации;

–выкладывает акции протеста с плакатами пацифистской направленности, осуждающие действия России и политику Президента Российской Федерации;

–дискредитирует ВС РФ;

–организовывает сбор денежных средств в том числе и на электронные крипто-кошельки, на нужды Легиона «Свобода России» (Подразделение ВСУ, сформированное из военнопленных и добровольцев перешедших на сторону Украины).

Документировалась по средством анализа платформ блокчейн, запросов в компетентные органы и использования средств перегрузке трафика при отправке на криптокошелек.

Примером № 2 может служить деятельность самопровозглашённого публициста Петрова Л.В., который имея в социальной сети «Вконтакте» страницу размещал статьи дискредитирующие Вооруженные силы Российской Федерации, публично распространял заведомо ложную информацию об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации.

В ходе ведения ДОУ в отношении фигуранта, он был привлечен к административной ответственности предусмотренной ст. 20.3.3 КоАП РФ, ему назначен штраф в размере 30000 рублей, позже в отношении него было возбуждено уголовное дело по ч. 1 ст. 207 УК РФ, которое в настоящее время находится на рассмотрении в Горячеключевском городском суде.

При документировании преступления предусмотренного ч. 1 ст. 207.3 УК РФ, из основных доказательственных материалов был ответ из Министерства обороны о ложности сведений изложенных в публикации, наличие лингвистического исследования, получение информации по IP-адресу выделяемому абоненту в момент размещения публикации.

Политический экстремизм в регионах: примером может служить деятельность лица ведущего в мессенджере телеграмм канал «Протестный Геленджик», в котором разместил заведомо ложную информацию об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации.

ОРМ используемы при документировании основывались на методе поиска первичной информации в открытых сегментах сети Интернет, то есть интернет-мониторинг и как его разновидность – оперативно-розыскной мониторинг, который представляет собой комплексную систему оперативно-розыскных мероприятий направленную на идентификацию лица в сети интернет

Еще одним способом документирования стало использование методов анализа большого количества неструктурированных данных, известных как технология «Большие Данные». Их кардинальным отличием от оперативно-розыскного мониторинга, является осуществление поиска, анализа, и выявления криминальной социальной активности в сети Интернет не сотрудником, а с использованием автоматизированного программного обеспечения, позволяющего производить сбор, хранение и анализ данных по всей сети Интернет.

Экстремизм среди подростков «Сваттинг», ЧВК «Редан»: Любителей Анимэ, движение зародившееся 18.02.2023 в Москве группа т.н. неформалов пришла в ТЦ «Авиапарк» в фудкорт поесть, сидели ни кого не трогали

их заметили гопники, которые от скуки захотели докопаться и избить представителей субкультурного движения, но неожиданно для них получили жесткий отпор, который был заснят на камеру мобильного телефона одним из т.н. неформалов провозгласившие себя ЧВК «Редан». Видео быстро разлетелось по соц. сетям и группам в мессенджерах, получило много обсуждений и комментариев.

В последствии в сети Интернет представители ЧВК «Редан» и представители т.н. «Правых» отыскивали друг друга и договаривались о встрече с целью вступить в поединок т.н. «стенка на стенку»

Данные правонарушения необходимо пресекать до сбора участников путем мониторинга сети Интернет, и проведения оперативного внедрения в сети Интернет в деструктивные группы и последующей координации наружными нарядами полиции.

Увеличились случае вовлечения несовершеннолетних в акты ложного минирования(сватинга) путем использования IP телефонии и написанного заранее голосового сообщения или использование однодневных почт и почт созданных на ресурсах Теневого Интернета.

Эффективность проверки первичной информации о преступлениях складывается, в первую очередь, из компетенции оперуполномоченного, знания им информационных технологий. Современные реалии таковы, что сотрудник оперативного подразделения должен владеть компетенциями не только в своей профессиональной деятельности, но и в высокой степени быть носителем информационной культуры, уверенно владеющим современными информационными технологиями. Поэтому, решение вышеуказанных проблем, таких как своевременное реагирование на совершаемые преступления, возможно лишь при осуществлении постоянного информационного и аналитического поиска по имеющимся в доступе сетям. Для выработки новых методик документирования преступлений, совершаемых с использованием информационных технологий, необходимо переосмыслить типовые решения и сложившиеся схемы как в оперативно-розыскной, так и уголовно-процессуальной практике деятельности правоохранительных органов, переосмыслить содержание классических оперативно-розыскных мероприятий, а, это значит, начать по новому мыслить при планировании и разработке оперативных комбинаций, мыслить категориями информационных технологий.

Литература

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993).

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ

3. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ.

4. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 №174-ФЗ.

5. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

6. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности».

7. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

8. Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении».

9. Федеральный закон от 11 июля 2001 г. № 95-ФЗ «О политических партиях».

10. Федеральный закон от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях».

11. Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях».

12. Федеральный закон от 19 июля 2004 г. № 54 «О собраниях, митингах, демонстрациях, шествиях и пикетированиях».

13. Федеральный закон от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».

14. Федеральный закон от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию».

15. Федеральный закон от 12 января 1996 г. № 7-ФЗ «О некоммерческих организациях».

16. Постановление Правительства РФ от 18.01.2003 № 27 «Об утверждении Положения о порядке определения перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, и доведения этого перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом».

17. Постановление Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации».

18. Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности».

19. Постановление Пленума Верховного Суда РФ от 10.06.2010 № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)».

Частикова Вера Аркадьевна,
кандидат технических наук, доцент,
доцент кафедры кибербезопасности и защиты информации
Кубанского государственного технологического университета

Гуляй Виктория Геннадьевна,
студентка Кубанского государственного
технологического университета

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ ДАКТИЛОСКОПИЧЕСКИХ СКАНЕРОВ ПУТЕМ ПРИМЕНЕНИЯ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ

Аннотация: В статье рассмотрен алгоритм улучшения изображений отпечатков пальцев, получаемых на контрольно-пропускных пунктах, путем применения генеративно-состязательных нейронных сетей (GAN) в том числе с целью сокращения и предотвращения террористических актов в государственных учреждениях.

Ключевые слова: информационная безопасность, терроризм, экстремизм, биометрия, отпечаток пальца, папиллярный узор, нейронная сеть.

В современном мире с каждым годом растет число террористических преступлений. Регулярно поступают сведенья о предотвращенных террористических актах в школах, высших учебных заведениях, больницах и других общественных местах [4]. Все это свидетельствует об актуальности создания систем предотвращения экстремистских атак в обществе.

Так, сокращение времени, требуемого для обнаружения и привлечения к ответственности лиц, причастных к совершению террористических актов, может способствовать уменьшению числа совершаемых преступлений. С этой целью необходимо вести контроль всех лиц, посещающих государственные учреждения [3].

Одним из способов фиксации всех посетителей является внедрение пропускных пунктов, содержащих в себе автоматизированные системы аутентификации лиц, входящих и выходящих из зданий государственных учреждений [4].

Аутентификацию с помощью автоматизированных информационных систем можно проводить либо путем проверки знания секретного ключа (ввод пин-кода) или наличия объекта доступа (электронного ключа, карточек доступа), либо с помощью сверки биометрических данных.

Первый способ, представляющий собой классические схемы аутентификации субъектов доступа в виде ввода пароля и/или прикладывания электронного ключа, является весьма уязвимым. Так, с помощью алгоритмов социальной инженерии существует высокая вероятность утечки данных, т.е. пароль может быть передан третьим лица или подсмотрен непосредственно злоумышленниками [5].

Также при часто меняющихся посетителях, например, в больницах и поликлиниках, невозможно внедрить систему аутентификации, представляющую собой проверку пин-кода, так как такие данные в ближайшее время перестанут быть секретными, и система перестанет выполняет свою непосредственную функцию – ограничение доступа и аутентификация личности.

Такие системы уместны только в тех учреждениях, которые посещает примерно один и тот же круг лиц, например, образовательные учреждения. Однако, в таких местах, зачастую наблюдается большое скопление людей, приходящих к определенному времени. Учитывая, что на ввод пароля требуется определенное время, то такая система аутентификации будет провоцировать давку, что будет вызовет недовольство людей и создаст еще большую угрозу террористических актов. Поэтому в таких организациях все чаще переходят на аутентификацию с помощью электронных ключей.

Однако, путем различных техник социальной инженерии подготовленному злоумышленнику не составит труда заиметь такой объект доступа [5]. Например, притворившись студентом, опаздывающим на очень важный экзамен, попросить карточку-допуск у одного из стоящих рядом с выходом студентов и таким образом проникнуть в здание университета. Также такие карточки доступа, как и другие электронные ключи, часто теряются, что идет только на пользу преступникам.

Наиболее надежным является другой способ обеспечения ограниченного доступа и контроля – внедрение биометрических систем аутентификации [2]. Биометрические данные, как объект доступа, невозможно потерять, передать третьим лицам и т.д. Также такие системы не только подтверждают доступ определенных лиц, но и фиксируют их личность.

Согласно Федеральному закону от 29.12.2022 № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" сбор и хранение биометрических данных будет производится государством, что способствует внедрению систем, базирующихся на идентификации личности с помощью биометрических данных.

С момента вступления данного закона [7] в силу государственные организации смогут осуществлять разграничение доступа с помощью различных систем биометрической идентификации, например, сканеров отпечатков пальцев. Сведенья, получаемые при сканировании на пункте пропуска в организации будут сверяться с данными, внесенными в государственный реестр биометрических данных – «Единая биометрическая система». Это облегчит внедрение биометрических систем доступа в организации, так как упростит процесс снятия первоначальных биометрических данных и обеспечения безопасности их хранения [2].

Внедрение таких систем позволит не только ограничить проникновение лиц, не имеющих доступа в данные организации, но и зафиксировать личности всех, кто входил и выходил из учреждения [2].

Одним из наиболее надежных и легко внедряемых видов биометрических систем являются дактилоскопические сканеры. Сканеры отпечатков пальцев или дактилоскопические сканеры представляют устройства фиксации элементов папиллярного узора кончиков пальцев рук человека [1].

Применение таких устройств имеет ряд преимуществ:

1. папиллярный узор не изменяется в течении жизни человека и восстанавливает до первоначального состояния после травм, что позволяет использовать одно и то же прототипное изображение на протяжении долгого времени;

2. такие системы имеют низкую стоимость установки и дальнейшего обслуживания, а также не требуют закупки дополнительных устройств, обеспечивающих доступ в помещения (например, электронный ключ для каждого человека, имеющего доступ в здание).

Однако, при большом потоке людей, прикладывающих палец к устройству, на панели сканера достаточно быстро появятся частички грязи, влаги и других инородных веществ, что может сказаться на качестве распознавания папиллярного узора [1].

Для избежания снижения эффективности работы дактилоскопических сканеров в системы биометрической аутентификации, работающих с отпечатками пальцев, следует применять специализированное программное обеспечение [6], позволяющее не терять качество получаемых изображений независимо от наличия или отсутствия инородных тел на панели сканера.

В частности, для достраивания недостающих фрагментов папиллярного узора и повышения качества изображений, получаемых с помощью дактилоскопических сканеров, следует использовать интеллектуальные системы, базирующиеся на генеративно-состязательных нейронных сетях (GAN-сети).

Применение GAN-сетей позволит повысить функциональную эффективность дактилоскопических сканеров [6]. Генеративно-состязательные нейронные сети представляют собой систему двух сетей, одна из которых (генератор) на основе поступающих на вход ключевых признаков создает изображения, а вторая (дискриминатор), получая на вход реальные и сгенерированные изображения, определяет какие из изображений – искусственно созданные. Если дискриминатору удалось отличить сгенерированные изображения от реальных, то генератор вновь обучается на новых данных и создает изображения до тех пор, пока дискриминатор не сможет отличить их от настоящих. Такая система позволяет достраивать изображения отпечатков пальцев и помогает избегать ошибок идентификации, возникающих при попадании инородных тел на панель дактилоскопических сканеров.

Литература

1. Ващенко, Л. С. Дактилоскопия как один из способов установления личности / Л. С. Ващенко, Е. В. Козликина // Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений : Сборник научных статей по итогам работы круглого стола №5 со Всероссийским и международным участием, Шахты, 30–31 мая 2021 года / УКК «Актуальные знания»; Ассоциация «Союз образовательных учреждений». Том Часть 1. – Шахты: Общество с ограниченной ответственностью "КОНВЕРТ", 2021. – С. 151-152. – EDN ZNGUZM.

2. Степанов, И. В. Системы контроля управления доступом по биометрическим параметрам / И. В. Степанов, Д. И. Стукань, А. Ю. Воднев // СОВРЕМЕННАЯ НАУКА и МОЛОДЫЕ УЧЁНЫЕ : сборник статей VIII Международной научно-практической конференции, Пенза, 12 января 2022 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 42-45. – EDN HPTOBW.

3. Тыныбаев, А. Н. Противодействие терроризму и религиозному экстремизму в информационном пространстве / А. Н. Тыныбаев, Р. С. Иржанов // Мировой политический процесс: информационные войны и «цветные революции»: Сборник материалов Международной научно-практической конференции, Москва, 27–29 октября 2021 года. – Москва: Московский государственный лингвистический университет, 2022. – С. 216-221. – EDN GIFFNC.

4. Усманова, Р. М. Международный терроризм как угроза национальной безопасности / Р. М. Усманова, Л. А. Исаева // Право и государство: теория и практика. – 2022. – № 1(205). – С. 205-207. – DOI 10.47643/1815-1337_2022_1_205. – EDN CSIVEX.

5. Частикова, В. А. Методика обнаружения атак социальной инженерии на основе алгоритмов анализа естественного языка / В.А. Частикова, В.Г. Гуляй // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 3(59). – С. 61-71. – DOI 10.54398/20741707_2022_3_61. – EDN EEOXVM.

6. Частикова, В. А. Нейросетевой подход к решению задачи построения фоторобота по словесному описанию / В. А. Частикова, С. А. Жерлицын, Я. И. Воля // Известия Волгоградского государственного технического университета. – 2018. – № 8(218). – С. 63-67. – EDN XYKSJV.

7. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

Частикова Вера Аркадьевна,
кандидат технических наук,
доцент кафедры кибербезопасности и защиты информации
Кубанского государственного технологического университета

Хлыст Даниил Александрович,
студент Кубанского государственного
технологического университета

ОБЗОР СУЩЕСТВУЮЩИХ РЕШЕНИЙ СИСТЕМ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В данной статье проведен обзор наиболее популярных решений класса IRP на российском рынке. Рассмотрены продукты Jet Signal, R-Vision Incident Response Platform, Security Vision Incident Response Platform, CyberBit SOC 3D, IBM, Fast Incident Response (FIR), The Hive, Makves IRP, NextSTage IRP, ThreatFusion. В работе описаны особенности каждой системы, их достоинства и недостатки.

Ключевые слова: Информационная безопасность, система реагирования на инциденты, расследование инцидентов.

Современные компании всё больше используют решения класса IRP, чтобы оперативно реагировать на информационные инциденты и сохранять безопасность своих данных. Выбор правильного IRP-инструмента играет важную роль в защите информации организации, ведь это неотъемлемая часть для создания ситуационного центра информационной безопасности[12]. В данной статье рассмотрены наиболее популярные решения класса IRP на российском рынке[1].

Рис. 1. Структура центра мониторинга информационной безопасности

1.Jet Signal – платформа для обработки кибератак, разработанная российской компанией. Она позволяет обнаруживать и реагировать на кибератаки на ранней стадии, а также отслеживать множество типов угроз, включая DDoS и APT. Jet Signal обладает несколькими преимуществами, включая[2]:

– высокая скорость реагирования на угрозы;

– хорошая масштабируемость;

– доступность на российском рынке.

Недостатком Jet Signal является то, что ее стоимость высока, что делает ее недоступной для малых и средних компаний. Также она не обладает всеми возможностями, которые имеют более дорогие аналоги на рынке.

2. R-Vision Incident Response Platform (R-Vision SOAR) [3] этот продукт отличается высоким уровнем интеграции с различными информационными системами, что позволяет обеспечить быстрое реагирование на инциденты. Однако. Стоимость на данное решение не приводится, так как она зависит от многих факторов. R-Vision Incident Response Platform – это инструмент для обработки и реагирования на кибератаки. Он позволяет обнаруживать угрозы на ранней стадии, а также оценивать уровень угрозы. R-Vision обладает следующими особенностями:

– хорошие средства фильтрации и анализа;

– высокая скорость реагирования на угрозы;

– расширенный функционал взаимодействия с ГосСОПКА;

– наличие готовых скриптов реагирования;

– поддержка различных типов устройств на рынке;

– лицензия поставляет комплектами с разным функционалом.

Одним из недостатков R-Vision это то, что данный продукт не так прост в использовании, и может потребоваться дополнительная подготовка персонала. Также в схеме лицензирования данной системы не учитываются внешние системы заказчика. Кроме того, любая кастомизация предполагает затраты с каждой из сторон, поэтому запросы на добавление функциональности решения определенно будут учтены, но могут быть не приняты без дополнительной оплаты.

3. Security Vision Incident Response Platform[4] – имеет мощные средства анализа и мониторинга, что позволяет более эффективно защищать информационные системы. Обладает несколькими преимуществами, включая:

– хорошие средства автоматизации реагирования на угрозы;

– высокая скорость обработки;

– добавление виджетов в инциденты;

– платформа-конструктор для удобной настройки под собственные бизнес задачи;

– встроенные механизмы корреляции получаемой информации от внешних систем;

– автоматический анализ ранее случившихся инцидентов безопасности для принятия новых решений.

4. CyberBit SOC 3D – это современная система, которое позволяет не только быстро обнаруживать и реагировать на инциденты, но и предоставляет уникальные возможности по обучению персонала в области кибербезопасности. CyberBit SOC 3D обладает богатым функционалом, однако достаточно сложна в использовании. Система обладает несколькими преимуществами, включая:

– синергия с другими продуктами cyberbit;

– автоматизирует сбор индикаторов компрометации со всей цифровой базы клиента;

– автоматизирует расследование и сортировку инцидентов с использованием аналитики на основе больших данных;

– автоматизирует процессы с помощью готовых или создаваемых пользователем playbook.

5. IBM Resilient Incident Response Platform[5] – одно из наиболее известных платформ на рынке. Оно интересно своей универсальностью и совместимостью со многими другими продуктами IBM. Кроме того, IBM имеет большое сообщество пользователей, которые обмениваются опытом в использовании данного IRP. Основным недостатком IBM можно считать его высокую цену.

6. Fast Incident Response (FIR) – это относительно новый продукт, которое нацелено на малые и средние предприятия. FIR легко устанавливается и настраивается, что позволяет его быстро использовать после установки. Кроме того, данный IRP поддерживает большое количество источников данных. Однако, по сравнению с некоторыми другими продуктами, FIR имеет более ограниченный функционал. Преимущества:

– простота обучения персонала;

– нет необходимости покупать лицензию;

– открытый код.

7. The Hive [6] – решение, которое отличается от других IRP своей открытостью и возможностью использования различных плагинов. The Hive имеет простой интерфейс для работы, но может потребовать дополнительной настройки для максимальной эффективности. Преимущества:

– открытый код;

– быстрое развитие;

– интеграция с любым внешним источником;

– нет необходимости покупать лицензию.

8. Makves IRP[7,8] — это инструмент управления угрозами, который обеспечивает непрерывное мониторинг сетевого трафика, а также быстрый анализ и реакцию на потенциальные угрозы. Makves IRP обеспечивает полный контроль над потоком данных и позволяет быстро реагировать на нарушения безопасности. Обладает несколькими преимуществами, включая:

– быстрый поиск инцидентов;

– простой и удобный интерфейс;

– журнал аудита как от системы, так и от пользователя;

– использование технологии машинного обучения.

Данное решение позиционирует себя как простой и удобный инструмент для регистрации инцидентов, управления их жизненным циклом. Однако, в нем отсутствует аварийное восстановление, управление расследованиями и задачами.

9. NextSTage IRP – отличается своей высокой гибкостью и способностью быстро реагировать на новые угрозы. Кроме того, NextSTage IRP автоматически группирует инциденты, что упрощает работу персонала. Однако, среди недостатков можно отметить его несколько ограниченную функциональность.

Особенность:

– расширенные возможности no-code;

− возможность кастомизации;

– гибкие архитектурные возможности;

– возможность настройки playbook для разных типов инцидентов;

– взаимодействие с ГосСОПКА.

К сожалению, оповещение о реагировании происходит только по e-mail, когда другие решения позволяют использовать СМС, мессенджеры, RSS. Также нет возможности запуска нескольких сценариев в одном инциденте.

10. ThreatFusion [9] — это решение, которое используется для обнаружения и классификации инцидентов информационной безопасности. это инструмент реагирования на инциденты и расследования угроз. Это отличный инструмент для предоставления данных об угрозах в режиме реального времени и поиска сложных деталей. Программное обеспечение предоставляет пользователям большое преимущество, получая данные из глубокой сети и даркнета для выявления любых утечек данных.

Особенность:

– легкая интеграция

− вывод угроз и управление IOC;

– сбор данных из многих частей интернета;

– инструмент использует искусственный интеллект для поиска данных из различных источников для выявления угроз.

IRP – это неотъемлемый элемент защиты информационной системы, который позволяет быстро и эффективно реагировать на инциденты. На рынке существует множество различных решений, каждое из которых обладает своими преимуществами и недостатками. Важно учитывать, что IRP должен интегрироваться с другими системами безопасности для обеспечения эффективной защиты, цена также может быть фактором, который отра-

зится на доступности продукта для многих организаций [12]. Выбор конкретного продукта зависит от многих факторов, включая бюджет, специфику бизнеса и дополнительные требования к функционалу.

Литература

1. Обзор рынка платформ реагирования на инциденты (IRP) в России. – 2018. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia
2. Система управления инцидентами информационной безопасности Jet Signal. – Режим доступа: https://jet.su/about/directions/informatsionnaya-bezopasnost/
3. Система оркестрации, автоматизации ИБ и реагирования на инциденты R-Vision SOAR. – Режим доступа: https://rvision.ru/products/soar
4. Security Vision Incident Response Platform (IRP / SOAR). – Режим доступа: https://www.securityvision.ru/products/irp/
5. Обзор IBM Resilient Incident Response. – Режим доступа: https://expertinsights.com/reviews/ibm-resilient-incident-response
6. Бесплатная IRP-система своими силами: опыт использования платформы с открытым кодом The Hive. – 2019. – Режим доступа: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own
7. MAKVES IRP универсальная система для регистрации и учета инцидентов). – Режим доступа: https://makves.ru/irp/
8. IRP/SOAR: автоматизация управления инцидентами – 2022 – Режим доступа: https://www.itsec.ru/irp-soar
9. Top 32 Incident Response Tools. – 2022 – Режим доступа: https://startupstash.com/incident-response-tools/
10. Системы реагирования и управления инцидентами информационной безопасности (IRP) – Режим доступа: https://www.anti-malware.ru/security/irp
11. Частикова В.А., Жерлицын С.А., Воля Я.И., Сотников В.В. Нейросетевая технология обнаружения аномального сетевого трафика // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 20-32.
12. Козырь Н. С. Вопросы эвентуальности цифровой трансформации социально-экономических систем // E-Management. 2023. Т. 6. № 1. С. 51-60. – DOI 10.26425/2658-3445-2023-6-1-51-60
13. Chastikova V.A., Sotnikov V.V. Method of analyzing computer traffic based on recurrent neural networks // Journal of Physics: Conference Series. International Conference «High-Tech and Innovations in Research and Manufacturing», HIRM 2019. 2019. С. 012133.
14. Седых Н. В., Фоканов И. П. Проблемы и перспективы развития технологии искусственного интеллекта // Естественно-гуманитарные исследования. 2022. № 44(6). С. 266-267.

Жерлицын Сергей Анатольевич,
аспирант Кубанского государственного
технологического университета

ИНЖЕНЕРНЫЕ РЕШЕНИЯ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО РИСУНКУ ВЕН ЛАДОНИ

Аннотация: Представленная статья описывает технологию идентификации личности по рисунку вен ладони с использованием инфракрасного излучения и нейросетевых алгоритмов. В рамках исследования была разработана система, состоящая из веб-камеры без инфракрасного фильтра, светодиодного освещения и специального корпуса. Применение метода потокового сканирования и анализа множества сканов позволяет эффективно устранять шумы и выбросы, обеспечивая более надежную и точную идентификацию личности. Разработанные инженерные решения значительно повышают надежность системы, минимизируют вероятность ошибочной идентификации и обеспечивают высокую эффективность процесса идентификации на основе рисунка вен ладони.

Ключевые слова: Искусственный интеллект, нейронная сеть, информационная безопасность, идентификация личности, рисунок вен ладони.

Введение

Вопросы безопасности и эффективности идентификации личности становятся все более значимыми в различных отраслях. В связи с этим возникает повышенный интерес к использованию рисунка вен ладони в качестве биометрического идентификатора [1]. Этот подход обладает рядом преимуществ, делающих его предпочтительным по сравнению с традиционными методами идентификации.

Прежде всего, важно отметить, что невозможность переиздать биометрический идентификатор в случае его компрометации, делает дополнительный параметр необходимым и актуальным. Это существенно для обеспечения долгосрочной безопасности защищаемых систем.

Кроме того, невозможно скопировать рисунок вен ладони незаметно и без прямого воздействия на субъект. Это увеличивает уровень безопасности системы идентификации и значительно затрудняет возможные спуфинг-атаки.

Другим важным преимуществом является эргономичность и простота применения данного метода. Считывание рисунка вен ладони может быть выполнено быстро и без необходимости особых навыков со стороны пользователя на специальном устройстве. Это упрощает процесс идентификации и обеспечивает удобство для конечных пользователей.

Одним из дополнительных преимуществ идентификации по рисунку вен ладони является ее гигиеничность. Бесконтактная реализация этого метода делает его особенно ценным в условиях, когда гигиена и избежание контактов с поверхностями приобретают особую значимость, например, во время эпидемических вспышек.

Цель данной научной статьи состоит в исследовании и разработке инженерных решений, направленных на повышение точности идентификации личности по рисунку вен ладони. В этом контексте научная новизна проекта проявляется в применении передовых нейросетевых технологий, актуальных алгоритмов машинного обучения и использовании современных библиотек и фреймворков в области машинного обучения и компьютерного зрения [2].

Ранее предложенная технология не использовалась для решения поставленной задачи идентификации по рисунку вен ладони, в то время как существующие аналоги опираются на устаревшие методы анализа идентификаторов. Результаты патентного поиска подтверждают несоответствие существующих аналогов современным требованиям и методологии.

Общее описание системы

В данном исследовании представлена технология идентификации личности по рисунку вен ладони, основанная на использовании инфракрасного излучения и нейросетевых алгоритмов. Аппаратная составляющая системы включает веб-камеру с вручную удаленным инфракрасным фильтром, светильник с семью светодиодами ближнего инфракрасного диапазона и специальный корпус. Прототип прибора приведен на рисунке 1.

Рис. 1. Прототип прибора

Светодиоды, излучая невидимый для глаза свет с длиной волны 850 нанометров, позволяют формировать рисунок вен на ладони. Это происходит благодаря поглощению инфракрасного излучения гемоглобином крови. В результате поглощения, вены становятся видимыми на изображении, представляя собой черные линии. Пример полученного таким образом изображения приведен на рис. 2.

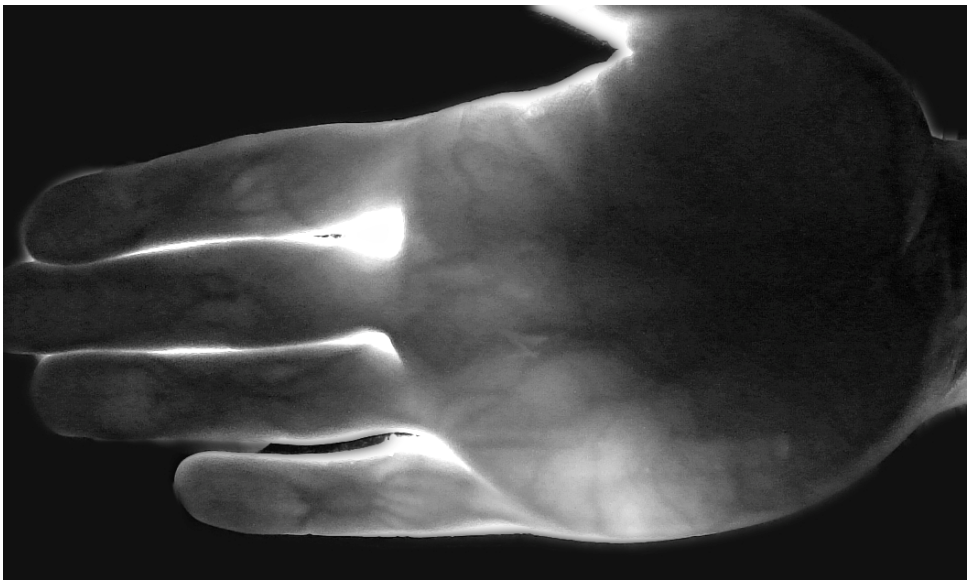


Рис. 2. Снимок рисунка вен ладони в инфракрасном свете

Для анализа полученных изображений был применен нейросетевой аппарат. Методика идентификации была реализована в трех различных вариантах: на основе бинарной классификации, категориальной классификации и комбинированный [3].

В результате экспериментов была разработана нейросетевая архитектура, включающая чередующиеся сверточные слои и слои субдискретизации. Результат последнего субдискретизирующего слоя подается на два полносвязных слоя, которые выполняют конечную классификацию.

Предложенная технология представляет собой инновационное решение, где комбинация инфракрасной техники и нейросетевых алгоритмов обеспечивает точность и надежность идентификации личности по рисунку вен ладони.

Однако, в силу особенностей работы применяемых алгоритмов и аппаратной реализации, система требует определенных усовершенствований для достижения более высокой эффективности и точности идентификации по рисунку вен ладони [4]. В этом контексте, предлагаемые инженерные решения призваны решить следующие проблемы.

Минимизация влияния шумов в выходных данных

В предлагаемой системе идентификации личности по рисунку вен ладони используется потоковая работа сканера с целью преодоления шумов и выбросов, которые возникают в выходных данных из-за особенностей устройства и воздействия человеческого фактора. Этот подход основан на проведении последовательных сканирований ладони с высокой частотой, составляющей 20 сканирований в секунду. Каждое сканирование ладони сопровождается анализом полученных изображений при помощи нейросети.

Путем потокового сканирования и последующего анализа множества сканов система способна компенсировать и устранить шумы и выбросы, ко-

торые могут возникать в отдельных сканированиях. Такой подход обеспечивает более надежную и точную идентификацию личности по рисунку вен ладони. Для подтверждения достоверности идентификации необходимо достичь стабильного результата, подтвержденного последовательными согласованными результатами в течение 5 сканирований. Такое условие стабильности идентификации повышает достоверность системы и снижает вероятность ложных срабатываний.

В отсутствие потокового сканирования и анализа множества результатов система будет более подвержена влиянию шумов и выбросов в данных [5, 6]. Это может привести к ошибочной идентификации и привести к нежелательным ситуациям, например, предоставлению доступа несанкционированному лицу или отказу в доступе законному пользователю. Таким образом, использование потокового сканирования с анализом множества сканов повышает надежность и точность системы идентификации личности по рисунку вен ладони.

Повышение вычислительной эффективности

В силу ограничений и требований к производительности, непрерывное сканирование и анализ каждого кадра ладони может потреблять значительное количество вычислительной мощности и времени. Для оптимизации вычислительных ресурсов и снижения нагрузки на систему, в предложенной системе применяется простой и эффективный триггер, который активирует нейросетевой аппарат только при обнаружении ладони в устройстве. Для этого используется среднее значение яркости пикселей на считываемом изображении. Активация триггера происходит только при превышении заданного порогового значения яркости.

Использование такого примитивного триггера значительно экономит вычислительные ресурсы, так как нейросетевой аппарат активируется только в случае обнаружения ладони, а не постоянно работает на всем доступном видеопотоке. Это позволяет снизить нагрузку на вычислительные ресурсы системы и повысить ее общую эффективность. Более того, такой триггер является простым в реализации и не требует сложной настройки или высоких вычислительных затрат.

В отсутствие применения указанного триггера, система без использования данного метода будет непрерывно сканировать и анализировать видеопоток, что приведет к избыточным вычислительным затратам и неоправданному расходу ресурсов [7,8]. Поэтому использование простого триггера, основанного на яркости пикселей, позволяет оптимизировать работу системы и снизить нагрузку на вычислительные ресурсы.

Заключение

В данной научной статье были представлены инженерные решения, направленные на повышение точности идентификации личности по рисунку вен ладони. Основная цель исследования заключалась в разработке эффективных методов, использующих современные нейросетевые технологии и алгоритмы машинного обучения, для достижения надежной и точной идентификации.

В ходе работы было продемонстрировано, что потоковое сканирование с множественным анализом позволяет компенсировать шумы и выбросы, которые могут возникать при сканировании ладони. Множественные сканирования с высокой частотой и последующий анализ с использованием нейросети позволяют улучшить надежность и точность идентификации, обеспечивая более стабильные результаты.

Также было показано, что использование простого триггера на основе анализа яркости позволяет оптимизировать вычислительные ресурсы системы. Активация сканирования и анализа ладони происходит только при наличии ладони в кадре, что снижает нагрузку на вычислительный аппарат и повышает эффективность системы.

Таким образом, исследование позволило разработать и предложить инженерные решения, которые способствуют повышению точности идентификации личности по рисунку вен ладони. В будущем возможно расширение данного исследования с целью улучшения и оптимизации предложенных методов и их адаптации для более широкого спектра прикладных областей.

Литература

1. Козырь Н. С. Вопросы эвентуальности цифровой трансформации социально-экономических систем // E-Management. 2023. Т. 6. № 1. С. 51-60. – DOI 10.26425/2658-3445-2023-6-1-51-60.

2. Седых Н. В., Фоканов И. П. Проблемы и перспективы развития технологии искусственного интеллекта // Естественно-гуманитарные исследования. 2022. № 44(6). С. 266-267.

3. Частикова, В. А. Нейросетевая методика идентификации личности по рисунку вен ладони / В. А. Частикова, С. А. Жерлицын // Известия ЮФУ. Технические науки. – 2022. – № 4(228). – С. 192-200. – DOI 10.18522/2311-3103-2022-4-192-200.

4. Частикова В.А., Жерлицын С.А., Воля Я.И., Сотников В.В. Нейросетевая технология обнаружения аномального сетевого трафика // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 20-32.

5. Jain A.K., Ross A. and Pankanti S. Biometrics: a tool for information security // Trans Inform Forensics Secur. – No. 1 (2). – P. 125-143.

6. Im S., Park H., Kim Y, Han S., KIm S., Kang C., Chung C. A Biometric identification system by extracting hand vein patterns // J Korean Phys Soc. – Vol. 28 (3). – P. 268-272.

7. Malatras A., Geneiatakis D. and Vakalis I. On the efficiency of user identification: a system-based approach // Int. J. Inf. Secur. – No. 16. – P. 653-671.

8. Chastikova V.A., Sotnikov V.V. Method of analyzing computer traffic based on recurrent neural networks // Journal of Physics: Conference Series. International Conference «High-Tech and Innovations in Research and Manufacturing». HIRM 2019. 2019. С. 012133.

Шайдаев Мирзабек Шайдаевич,
старший научный сотрудник
отдела координации и внедрения научно-технической продукции
Центра сопровождения научно-исследовательских
и опытно-конструкторских работ в области
информационных технологий
Научно-исследовательского института
специальной техники,
кандидат юридических наук
ФКУ НПО «СТиС» МВД России

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РУКАХ ТЕРРОРИСТОВ И ЭКСТРЕМИСТОВ КАК УГРОЗА БЕЗОПАСНОСТИ ГОСУДАРСТВА И ОБЩЕСТВА

Ускоренное развитие технологий искусственного интеллекта (ИИ) в настоящее время приводит к значительному расширению сферы его применения. Вместе с тем, удешевление, доступность и простота передачи программного обеспечения ИИ, изначально создаваемого с благими намерениями, не исключает вероятность злонамеренного его использования, в том числе в преступных целях. Искусственный интеллект в руках преступников становится эффективным средством для реализации своих преступных намерений, а в руках террористов и экстремистов, быстро берущих на вооружение всевозможные новые технологии, признается одной из угроз безопасности государства и общества. В эпоху цифровизации экстремизм и терроризм превращаются в главную опасность не только для России, но и для многих стран мира, поскольку использование цифровых технологий искусственного интеллекта, больших данных повышают эффективность их преступной деятельности [6].

При этом следует отметить, что несмотря на наблюдаемый рост этой масштабной угрозы, практически во всех этических кодексах искусственного интеллекта (ИИ), принимаемых в разных странах, о злонамеренном использовании искусственного интеллекта упоминается лишь мельком либо не упоминается вообще [4. С. 105].

Специалистами различается два вида рисков применения искусственного интеллекта: умышленное противоправное воздействие на человека, а также преднамеренное совершение искусственным интеллектом общественно-опасных деяний [2].

Большую опасность, в случае утраты полного или частичного контроля за искусственным интеллектом, представляет его использование для целевого высокотехнологичного информационно-психологического воздействия на людей, так как оно может быть оказано единовременно на большие ее массы. Экстремистским и террористическим идеологам использование

технологий искусственного интеллекта предоставляет широкий спектр инструментария для осуществления целевого информационно-психологического воздействия, в реализации которого специалистами отмечается несколько путей.

Так, в информационной сфере возможности искусственного интеллекта могут быть использованы для представления ложной информации или ложной интерпретации существующего факта общественной или политической жизни для провоцирования целевых групп на неадекватную реакцию.

С целью искусственного продвижения в медиапространстве необходимого контента (той или иной новости, персоны и т.п.) искусственный интеллект предоставляет возможность установки и закрепления необходимой повестки дня. Постоянно навязывая людям определенный контент, он начинает приобретать для них особую ценность и важность, тем самым облегчая процесс привлечения экстремистами и террористами новых сторонников в свои организации [7. С. 288].

Вариантом использования ИИ в Интернете может быть создание различного интерактивного программного обеспечения для общения с пользователями через социальные сети с целью изучения сферы их общения. Такое программное обеспечение – интеллектуальные агенты, обычно называемые «веб-роботами», «социальными» или «чат-ботами», наряду с общением выполняют функцию продвижения идей. В руках экстремистских организаций боты на основе ИИ быстро заменяют людей-пропагандистов, вербовщиков и наёмных троллей. Организации типа «Аль-Каиды» или «Исламское государство» имеют самые широкие сети в социальных сетях и, таким образом, представляют собой наиболее опасный и тревожный пример этой тенденции в глобальном масштабе. Обладая большим опытом в использовании механизмов социальной инженерии в своих психологических операциях запрещенная в России организация «Исламское государство» еще в 2015 году создала тысячи ботов в «Twitter» для пропаганды, сбора средств и вербовки, координации активных и потенциальных боевиков, а также для расширения своей аудитории среди активных пользователей существующих продуктов ИИ [4 С. 110-111].

Одновременно, следует отметить уязвимость создаваемых с благими намерениями «чат-ботов», связанную со способностью ИИ к самообучению и запоминанию. Эффекты обучения алгоритмов в значительной степени зависят от данных, на основе которых проводится обучение. Умышленным искажением данных (это называется «отравлением» данных) можно изменить работу алгоритма, навязывая в процессе общения с «чат-ботом» деструктивный контент и радикальные взгляды для направления его работы против общества, и нацелить ИИ на дальнейшую их пропаганду. Так случилось с чат-бот виртуальной девушкой по имени Тэй, которая через непродолжительное время стала выдавать экстремистские утверждения [3]. Распространение

упрощенных, недорогих или даже бесплатных ботов позволяет экстремистским организациям устанавливать аффективные связи с пользователями социальных сетей и мобилизовывать посредством их на радикальные и насильственные действия.

С использованием алгоритмов глубокого обучения возможно осуществление целевой трансформации обычных, повседневных образов, превращение их в страшные, зловещие картинки. Многократное и быстрое увеличение и дальнейшее направление вала негативных образов на целевые аудитории в любой точке мира, способно быстро подстроить ее под их скрытые и часто неосознанные ожидания, с целью увеличения эффективности воздействия.

Возможности искусственного интеллекта все шире используются для манипулирования мнениями журналистов, блогеров и т.п., а также их аудитории. Путем анализа с помощью искусственного интеллекта тональности текстов информационных источников (блоги, статьи, форумы, опросы и т.д.) определяется отношение автора текста к предмету, обсуждаемому в тексте [7, С. 282].

Создание глубинных фейков с использованием **технологий «фальшивых людей»** («fake people») позволяет генерировать поддельные видео публичных политиков, деятелей бизнеса и культуры, представителей конфессиональных организаций с сообщениями, способными спровоцировать напряженность. Например, **о**бученная самостоятельно генерировать изображения людей, нейросеть, основываясь на бесконечной коллекции изображений реальных лиц, за секунды может создать в большом разрешении изображения лиц несуществующих или реальных людей, добавлять любые культурные и этнические особенности, эмоции, настроения. На основе метода синтеза человеческого изображения и голоса («deepfake»), ИИ в дальнейшем может синтезировать изображение и голос человека [7. С. 287]. С такими технологиями, особенно если они будут с открытым кодом, возможно создание любого поддельного видео, практически не отличающегося от реального. К тому же, средний уровень доверия, который вызывают изображения людей, созданные ИИ, по результатам исследований Ланкастерского и Калифорнийского университетов установили на 7,7% выше, чем средний уровень доверия изображениям реальных людей [4]. Таким образом, возможно создание видеоизображений различных, в том числе известных лиц, для манипулирования поведением больших целевых групп. Например, убедив несовершеннолетних с помощью синтезированного видеообращения какого-нибудь их кумира посетить подложное законное мероприятие, вовлечь их в массовые беспорядки [1]. В другом случае возможно устройство провокаций, например, на религиозной или национальной почве.

Существенную опасность представляет попадание в руки террористов системы предсказательной аналитики на основе больших данных с использованием ИИ, которые обрабатывая данные СМИ и социальных сетей, могут

получать данные о будущих событиях, корректировать будущее из настоящего [7. С. 290]. Например, террористы, определив дату, место сбора протестующей группы населения или проведения марша несогласных, могут спланировать террористический акт во время подобных масштабных социальных выступлений[1].

В качестве примеров преднамеренного совершения искусственным интеллектом общественно-опасных деяний можно рассмотреть случаи захвата террористами контроля над искусственным интеллектом, входящим в различные системы управления, и переориентирование его на совершение необходимых для террористов действий. Так, например, з**ахват** контроля над системой управления беспилотным автомобильным транспортом в большом городе может привести к многочисленным жертвам, вызвать панику и создать психологический климат, который облегчит проведение других преступных действий [7. С. 284]. **Аналогично, захват** контроля над системой управления беспилотных летательных аппаратов может быть использован, например, с целью доставки взрывчатых веществ и создания технологических аварий [7. С. 286].

По мере совершенствования технических возможностей ИИ и растущего запроса на такие возможности со стороны экстремистских и террористических организаций не исключено создание новых синтетических информационных продуктов, основанных на комбинации техник психологического воздействия, сложных систем искусственного интеллекта и больших данных, могущих стать действенным инструментом оказания негативного воздействия на человека и массы.[2] Следовательно, на фоне нарастающего мирового кризиса, снижения уровня жизни основной части населения большинства стран, роста социальной и имущественной поляризации, опасного роста геополитического соперничества при наблюдающемся отставании осмысления человеком новых угроз, связанных с развитием технологий искусственного интеллекта, тенденция неуклонного роста новых случаев злонамеренного их использования будет продолжаться.

В складывающейся ситуации необходима консолидация усилий мирового сообщества по созданию предпосылок для устойчивого и безопасного развития человечества в условиях новых высокотехнологичных угроз обществу, в том числе создание соответствующих правовых, организационных и технических инструментов противодействия злонамеренному использованию искусственного интеллекта.

---

[1] Искусственный интеллект как террорист»: новые угрозы безопасности. Электронный ресурс: https://ria.ru/20190618/1555644961.html

[2] Искусственный интеллект и безопасность: что во благо, а что во зло? URL: https://interaffairs.ru/news/show/24219 (дата обращения 13.09.2022).

Литература

1. Багмет А. М., Бычков В. В. Расследование массовых беспорядков, в том числе с участием несовершеннолетних, и вовлечения в них несовершеннолетних: учеб. пособие. М. : ЮНИТИ-ДАНА, 2021. Электронный ресурс: URL: http://academy-skrf.ru/science/2021/Пособие-Расслед.массовых% 20беспорядков. pdf (дата обращения: 21.03.2023).

2. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 767–775. Электронный ресурс: URL: https://cyberleninka.ru/article/n/kriminologicheskie-riski-primeneniya-iskusstvenno go-intellekta (дата обращения: 21.03.2023).

3. Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-коммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. 2022 № 1. С. 60-65. Электронный ресурс: URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-kak-sredstvo-sovershеniya-prestupleniy-ekstremistskoy-napravlennosti-sovershennyh-s-ispolzo vaniem (дата обращения: 21.03.2023).

4. Матяшова Д.О. Злонамеренное использование искусственного интеллекта обсудили в рамках XIII международного IT-форума // Пролог: журнал о праве. – 2022. – № 2. – С. 105–114. – DOI: 10.21639/2313-6715.2022.2.12. Электронный ресурс: URL: https://cyberleninka.ru/article/n/ zlonamerennoe-ispolzovanie-iskusstvennogo-intellekta-obsudili-v-ramkah-xiii-mezhdunarodnogo-it-foruma (дата обращения: 21.03.2023).

5. Мосечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт- Петербургского университета. Право. 2019. Т. 10. Вып. 3. С. 461–476. Электронный ресурс: URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ugolovnaya-otvetstvennost-problemy-stanovleniya-novogo-vida-subekta-prestuplen iya (дата обращения: 21.03.2023).

6. Панкевич Т.В., Зубалова ГО.А. Современное состояние терроризма и экстремизма в условиях развития цифровых технологий // Юрист-Правоведъ. 2020 № 3(94). С. 64-68. Электронный ресурс: URL: https://cyberleninka.ru /article/n/sovremennoe-sostoyanie-ekstremizma-i-terrorizma-v-usloviyah-razvitiya-tsifrovyh-tehnologiy (дата обращения: 21.03.2023).

7. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // Государственное управление. Электронный вестник. 2019. Выпуск № 76. С. 279-303. Электронный ресурс: URL: https://cyberleninka.ru/article/n/zlonamerennoe-ispolzovanie-iskusstvennogo-intellekta-novye-ugrozy-dlya-mezhdunarodnoy-informatsionno-psihologicheskoy-bezopasnosti (дата обращения: 21.03.2023).

Шайдаев Мирзабек Шайдаевич,
кандидат юридических наук,
старший научный сотрудник отдела координации и внедрения
научно-технической продукции
Центра сопровождения научно-исследовательских
и опытно-конструкторских работ в области
информационных технологий
Научно-исследовательского института специальной техники
ФКУ НПО «СТиС» МВД России

СОЗДАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМУ МВД РОССИИ

С принятием в 1993 году Концепции развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью МВД России взяло неуклонный курс на внедрение и дальнейшее расширение применения информационных технологий на всех стадиях правоохранительной деятельности[1].

Повышение эффективности использования существующих в МВД России информационных ресурсов и обеспечение развития информационно-вычислительной системы МВД России как системы, интегрирующей информационные массивы органов внутренних дел на основе перспективных технологий их обработки, стало центральной линией Концепции развития информационно-вычислительной системы МВД России на 2002-2006 годы[2].

Принятой в 2006 году Программой МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» и внесенными в нее коррективами в 2008 году предприняты дальнейшие шаги по совершенствованию информационного обеспечения органов внутренних дел на основе оснащения их современными аппаратно-программными комплексами и системами, а также внедрению в практическую деятельность новых и перспективных информационных технологий[3].

Использование возможностей информационно-коммуникационных технологий для повышения эффективности своей деятельности было взято на вооружение оперативными подразделениями МВД России, в том числе

---

[1] Приказ МВД России от 12.05.1993 № 229 «О мерах по реализации Концепции развития информационного обеспечения органов внутренних дел«.

[2] Приказ МВД России от 13.06.2002 № 562 «Об утверждении Концепции развития информационно-вычислительной системы МВД России на 2002-2006 годы».

[3] Приказ МВД России от 20.05.2008 № 435 «Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел».

и Департаментом по борьбе с организованной преступностью и терроризмом (ДБОПиТ) МВД России.

В 2005-2008 годах разработаны и внедрены автоматизированные системы обработки информации о деятельности преступных сообществ и преступных групп, (шифр – «ПАУТИНА»), и обработки информации о результатах проведения оперативно-розыскных мероприятий (шифр – «Центр»). Предназначались они для осуществления ежесуточного сбора сведений о результатах работы, поступающих из территориальных подразделений по борьбе с организованной преступностью, для последующей их обработки и выработки управленческих решений по оптимальной расстановке, имеющихся у каждого конкретного подразделения кадровых и ресурсных возможностей.

Став правопреемником ДБОПиТ МВД России в 2008 году, Главное управление по противодействию экстремизму Министерства внутренних дел Российской Федерации (ГУПЭ МВД России)[1], продолжило курс по внедрению информационных технологий в деятельность своих подразделений.

С целью повышения качества информационной поддержки противодействия экстремистской деятельности в рамках компетенции МВД России (Центра «Э»), обеспечения возможности межведомственного сотрудничества в области противодействия экстремистской деятельности 17 апреля 2009 г. заключен государственный контракт на разработку автоматизированной информационной системы АИС «Экстремист».

Внедрение АИС «Экстремист» позволило обеспечить:

– создание базы данных по вопросам противодействия экстремистской деятельности;

– автоматизацию процессов обмена информационными фондами в рамках осуществления противодействия экстремистской деятельности между Центром «Э» МВД России и заинтересованными министерствами, и ведомствами;

– организацию в установленном порядке информационного взаимодействия с ФСБ и ФСО России.

На основе выбора оптимального базового программного продукта для создания приложения, функционал которого обеспечивает работу пользователей системы в режиме технологии клиент-сервер, реализованы возможности:

- ввода и коррекции информации, подлежащей учету в системе;
- формирования запросов по любой совокупности реквизитов для проведения последующего необходимого анализа отобранных сведений;

---

[1] Образовано в соответствии с Указом Президента Российской Федерации от 06.09.2008 № 1316 «О некоторых вопросах Министерства внутренних дел Российской Федерации». Новое наименование получило в соответствии с Указом Президента Российской Федерации от 01.03.2011 № 248 «Вопросы Министерства внутренних дел Российской Федерации».

– аналитической обработки с возможностью визуализации динамического изменения оперативной обстановки;

– обработки неструктурированной информации;

– аудита деятельности пользователей при работе с различными категориями информации;

– администрирования с широкими функциональными возможностями по систематизации сведений, содержащихся в базе данных и оптимизации процессов ее использования;

– оптимального представления сведений о субъектах экстремистской деятельности;

– формирования форм статистической отчетности;

– обмена информацией между различными уровнями территориального деления, принятыми в системе.

В настоящее время АИС «Экстремист» не соответствует уровню развития современных информационных и телекоммуникационных технологий и не позволяет выполнять требования, предъявляемые к информационным системам по обработке, хранению и информационному обмену сведениями, содержащие государственную тайну.

Для обеспечения оперативно-служебной деятельности ГУПЭ МВД России, а также выполнения требований, предъявляемых к информационным системам по обработке, хранению и информационному обмену сведениями, содержащими государственную тайну, планируется разработать сервис в составе ИСОД МВД России.

В 2019 году с целью повышения эффективности деятельности Главного управления по противодействию экстремизму Министерства внутренних дел Российской Федерации (ГУПЭ МВД России), подразделений ПЭ территориальных органов МВД России и подразделений, осуществляющих противодействие экстремизму, управлений на транспорте МВД России подготовлена заявка на выполнение опытно-конструкторской работы (ОКР) «Создание сервиса обеспечения деятельности Главного управления по противодействию экстремизму Министерства внутренних дел Российской Федерации», шифр «СОДГУПЭ». 17 июля 2020 года заключен государственный контракт на выполнение указанной ОКР.

Основываясь на результатах предыдущих опытно-конструкторских работ по автоматизации деятельности по линии борьбы с экстремизмом, разрабатываемый сервис предназначается для сбора, учета, обогащения поиска и агрегации информации, получаемой в рамках оперативно-розыскной деятельности и оперативно-розыскных мероприятий по вопросам противодействия экстремистской деятельности, содержащих сведения
о лицах, причастных к подготовке и совершению преступлений, фактах преступных проявлений посредством предоставления доступа к актуальной оперативно значимой информации в максимально короткие сроки.

Основные задачи, планируемые к выполнению сервисом:

– автоматизация процессов накопления, актуализация, поиск и обобщение информации, снижение трудозатрат на создание и поддержание в актуальном состоянии информационного фонда, оперативность доступа к информации по вопросам противодействия экстремистской деятельности;

– оптимизация и развитие процессов, связанных с аналитической обработкой информации, как находящейся в базе данных (БД) информационного фонда, так и поступающей в оперативном режиме из различных источников;

– выработка управленческих решений тактического и оперативного плана с помощью автоматизации процессов подготовки и принятия управленческих решений, планирования и контроля выполнения мероприятий ГУПЭ МВД России и курируемых им подразделений МВД России.

Функционирование СОДГУПЭ предполагается на федеральном и региональном уровнях.

Сервис представляет собой трёхуровневую информационную систему и двухконтурную учетную систему, соответствующую централизованной структуре ИСОД МВД России и взаимодействующую с другими сервисами ИСОД МВД России и внешними информационными системами.

Структурно сервис будет состоять из функциональных подсистем, предназначенных для реализации основных технологических задач по автоматизации процессов сбора, учета, обработки, представления и хранения данных, и обеспечивающих подсистем, необходимых для технологической поддержки работы функциональных подсистем.

Функциональные подсистемы предназначены для реализации следующих основных возможностей:

– автоматизация деятельности отделов ГУПЭ МВД России и курируемых им подразделений МВД России в рамках ведения сведений об объектах, представляющих оперативный интерес;

– обеспечение реализации функций контроля, целостности и сохранности информации на этапах получения, передачи, обработки, учета и хранения данных;

– поиск информации по произвольной совокупности;

– построение различных форм отчетности и визуализации данных, накапливаемых и обрабатываемых в СОДГУПЭ;

– обеспечение организации информационного обмена между подсистемами в составе сервиса, между сервисом и другими сервисами ИСОД МВД России, а также внешними информационными системами.

Технологические подсистемы предназначены для:

– управления учетными записями и настройки ограничения доступа пользователей к функциям и данным СОДГУПЭ;

– определения перечня сотрудников ГУПЭ МВД России и курируемых им подразделений МВД России, допущенных к работе в СОДГУПЭ;

– обеспечение реализации функций по предотвращению утечек, несанкционированного изменения, нарушения целостности и удаления данных.

Объектами учета разрабатываемого сервиса является информация о физических и юридических лицах, об организованных группах и преступных сообществах (преступных организациях), причастных к экстремистской и террористической деятельности, а также ее финансированию, о представляющих оперативный интерес связях указанных лиц (организаций), о выявленных фактах противоправных деяний, содержащихся в делах оперативно-розыскного производства, полученная в результате оперативно-розыскной деятельности.

Существенным сегментом в сервисе, обеспечивающим оперативность получения необходимых сведений и обмена информацией, является организация автоматизированного информационного взаимодействия с другими сервисами ИСОД МВД России, а также внешними информационными системами:

– сервисом обеспечения деятельности подразделений охраны общественного порядка (СООП) в части автоматизации процессов деятельности по обеспечению охраны общественного порядка;

– Федеральной информационной системой Госавтоинспекции МВД России (ФИС ГИБДД-М) в части получения/предоставления сведений о водителях, правонарушениях, транспортных средствах и их владельцах;

– сервисом обеспечения деятельности дежурных частей (СОДЧ) в части осуществления сбора, хранения и обработки и анализа оперативной информации, поступающей в дежурные части ТО МВД России, мониторинга оперативной обстановки, оперативного информирования иных территориальных органов и организации незамедлительного реагирования на сообщения о происшествиях и преступлениях;

– сервисом интегрированных банков данных федерального и регионального уровней (ИБД-Ф, ИБД-Р) для получения и представления пользователям сведений об интересующих объектах учета;

– сервисом управления доступом к информационным ресурсам и ресурсам (СУДИС) для обеспечения разграничения и управления доступом к информационным системам и ресурсам ИСОД МВД России;

– сервисом в сфере оказания государственных услуг в сфере миграции для накопления и обработки учетных данных, формируемых в процессе регистрационного учета граждан, регистрируемых по месту пребывания и по месту жительства в субъектах Федерации;

– единым информационно-расчетным центром (ЕИРЦ) г. Москвы в части получения сведений о начислениях и платежах за жилые и нежилые помещения, коммунальные и прочие услуги;

– автоматизированной информационной системой органов регистрации актов гражданского состояния (ЗАГС г. Москвы) в части хранения, анализа и обработки информационных данных и документов;

– автоматизированной информационной системой Пенсионного фонда Российской Федерации (ПФР) в части получения сведений об учете граждан в системе обязательного пенсионного страхования, организации и ведения сведений о каждом застрахованном лице;

– автоматизированной информационной системой ФНС России в части приема обработки, представления данных и анализа информации от налоговых органов.

К сожалению, в ходе опытно-конструкторской работы был разработан только технический проекта. Дальнейшее выполнение работы прекращено по причине расторжения государственного контракта в связи с невыполнением головным исполнителем обязательств по государственному контракту.

Вместе с тем, следует отметить, что потребность подразделений по противодействию экстремизму МВД России в создании подобного сервиса, как средства повышения эффективности их деятельности, продолжает быть весьма актуальной. Уже в том году в ФКУ НПО «СТиС» МВД России повторно поступила заявка на создание сервиса обеспечения деятельности ГУПЭ МВД России, что позволит решить насущные проблемы подразделений по противодействию экстремизму МВД России по обеспечению повседневной оперативно-служебной деятельности.

Литература

1. Указ Президента Российской Федерации от 06.09.2008 № 1316 «О некоторых вопросах Министерства внутренних дел Российской Федерации».

2. Указ Президента Российской Федерации от 01.03.2011 № 248 «Вопросы Министерства внутренних дел Российской Федерации».

3. Приказ МВД России от 12.05.1993 № 229 «О мерах по реализации Концепции развития информационного обеспечения органов внутренних дел».

4. Приказ МВД России от 13.06.2002 № 562 «Об утверждении Концепции развития информационно-вычислительной системы МВД России на 2002-2006 годы».

5. Приказ МВД России от 20.05.2008 № 435 «Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел».

Эль Зени Юсеф Андроник Мохамедович,
студент Санкт-Петербургского политехнического
университет Петра Великого

Чумакова Екатерина Сергеевна,
главный эксперт Экспертно-криминалистического центра
управления на транспорте МВД Российской Федерации
по Северо-Западному федеральному округу,
ассистент Санкт-Петербургского политехнического
университета Петра Великого

РАЗВИТИЕ КИБЕРПРЕСТУПНОСТИ ПРИ СОВЕРШЕНСТВОВАНИИ ЭЛЕКТРОМОБИЛЕЙ

Аннотация: Электромобили – перспективное направление в автомобильной индустрии. По статистике в некоторых регионах их продажи увеличились почти в 2 раза, соответственно выросло и производство. Они могут значительно улучшить экологию, а улучшение технологий их производства в теории позволят в будущем им быть доступными, удобными и способными проезжать большие дистанции на одном заряде. Также активно развивается внедрение цифровых компонентов в электромобили даже базовой комплектации, бортовые компьютеры становятся всё более и более функциональными, а возможность беспилотного управления машиной, казалось ещё недавно было предметом скорее научной фантастики, чем чем-то реальным, стало чем-то, что прямо сейчас проходит испытания в разных местах по всей планете.

Однако это открывает дополнительные возможности не только для пользователей данных транспортных средств, но в том числе и для злоумышленников, в частности тех, кто занимается непосредственно преступлениями в цифровой среде. Возможность дистанционного угона автомобиля пока остаётся художественным вымыслом, но это связано, скорее, с малым распространением подобных транспортных средств, чем его принципиальной невозможностью.

В данной работе будет рассмотрен возможный вектор развития киберпреступности касательно электромобилей, теоретические методы его противодействию и возможное развитие сферы в целом.

Ключевые слова: *электромобиль; кибербезопасность; киберпреступность; цифровой след; беспилотный транспорт; инновации; правила дорожного движения.*

Введение

Довольно бурное развитие технологий, начало которого можно обозначить ещё с прошлого века повлияло на все сферы жизнедеятельности че-

ловека, и разумеется транспортные средства не стали исключением, особенно выделяются из этого экологически чистые и начинённые последними веяниями технологий электрические автомобили.

Что интересно, повышенный интерес к данному средству передвижения начался сравнительно недавно, хотя электромобиль (точнее его прототип) появился раньше автомобиля на дизельном двигателе[1] – первый электромобиль в виде простой тележки с электромотором был создан ещё в 1841 году, а уже на международной выставке в Париже в ноябре 1881 года Густав Труве представил уже полноценный электромобиль.

Между 1881 годом и нашим временем прошёл солидный временной промежуток, за это время наблюдались определённые всплески интереса к машинам с электрическим двигателем, например в СССР 4 декабря 1978 года Ульяновский автомобильный завод выпустил опытную партию своеобразных электрогрузовиков, которые конструировались на основе УАЗ-451М [2].

Далее прошло затухание интереса к электромобилям, это было на фоне изменения цен на рынке нефтепродуктов [3], но вот в нашем 21 веке интерес снова «загорелся», вызвано это ростом цен на нефть в целом и повышением интереса к экологии и защите окружающей среды.

И в наше время бурного развития информационных технологий данные автомобили оказались начинены последними веяниями технологий, как в области разнообразного функционала бортового компьютера и интеграции его с разнообразными сервисами, так и новым вектором: беспилотным управлением.

Но, разумеется, это связано со многими сложностями, и способно привести к росту преступности в сфере автоугона, похищения личной информации и её дальнейшая эксплуатация в дурных целях.

Материалы и методы

Так как автопилот начал развиваться сравнительно недавно, заявлять о какой-либо объективности в этом вопросе пока рано, однако по уже собранной статистике можно сделать определённые выводы.

В данной работе использована статистика, а также новостные сводки относительно сферы электрических автомобилей, научные работы исследователей в этой сфере, а также доклады аналитических компаний и отчёты национальных транспортных служб.

Например, работа исследователей рынка и инвесторов Джеймса Арбиба и Тони Себы [4] указывает, что мы стоим на пороге самой быстрой и глубокой революции в сфере транспорта. Они предполагают, что рост цен на нефть приведёт к тому, что большая часть пассажиров будет использовать автономные электрические средства передвижения, которые будут находиться в собственности своеобразных «флотов», а не индивидов. Несмотря на огромные потери нефтяной индустрии и транспортных сервисов, это поможет сохранить деньги простым семьям (в конкретно данной работе речь идёт об американских семьях).

В числе проблем, с которыми подобная модель может столкнуться, упоминается и проблема баз данных, которая по мнению исследователей должна быть одновременно открытой и интероперабельной, то есть давать возможность разным системам взаимодействовать друг с другом и обмениваться информацией в угоду конкуренции и безопасности, но в то же время должна обеспечивать приватность, безопасные поездки и ответственность перевозчика.

В подобных ситуациях можно вспомнить массовые утечки баз данных пользователей того же Яндекса [5], но вопрос технической безопасности и предотвращение подобного рода взломов лежит полностью на владельцах подобных сервисов, государство со своей стороны же активно вмешиваться не должно, однако обязано создать правовую базу как основу для наказания и самих взломщиков, и владельцев сервисов, которые нарушают законодательство, а конкретно статьи 137, 274 и иные уголовного кодекса Российской Федерации[1] [6] и статью 13.11 Кодекса Российской Федерации об административных правонарушениях[2] [7].

Однако не только персональные данные под угрозой, в результате столь активного внедрения технологий в транспорт и отсутствия чёткого законодательства пострадать могут, в том числе, жизнь и здоровье человека.

Случай в марте 2018 года в города Тампа штата Аризона была зафиксирована первая смерть от беспилотного автомобиля [8]: Элейн Херцберг пересекала автостраду в неположенном месте и плохой освещённости, также она толкала вперёд велосипед и не смотрела на дорогу. В результате столкновения с автомобилем на базе Volvo XC90 который принадлежал компании Uber и на котором тестировалась система автопилота. Анализ показал, что в момент аварии система распознавания препятствий автомобилем успешно определила наличие объекта на пути движения, однако не смогла корректно классифицировать его тип и рассмотрела его сначала как неопознанный объект, затем как велосипедиста и только потом как автомобиль. Данный сбой системы объясняется тем, что в программное обеспечение был заложен слишком высокий порог распознавания опасных объектов, что было необходимо с целью отсеивания ложноположительных срабатываний. Кроме того, из отчета национального совета по безопасности на транспорте США [9] стало известно, что автомобиль имел возможность определить необходимость использования аварийных тормозов за 1,3 секунды до столкновения, однако данная функция была отключена инженерами компании Uber. Отключение системы аварийного торможения произошло в целях избежания

---

[1] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 28.04.2023).

[2] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 28.04.2023).

конфликтов управления и несанкционированного вмешательства со стороны водителя.

Но по итогам расследования виновной признали действия водителя, который мог бы среагировать на появление пешехода, однако этого не сделал. Интересно, что в том же отчёте упоминалось что пострадавшая находилось под действием наркотических веществ, однако вины водителя это разумеется не умаляет.

В данном случае стоит отметить, что законодательная база для подобных случаев попросту отсутствует, да, виновным признали в итоге водителя, а также стоит учитывать особенности американского права и роль в нём судебного прецедента. Но в Российской Федерации на данный момент тоже нет чёткого законодательства относительно беспилотных транспортных средств, разумеется, справедливо будет подметить, что это относительно молодая сфера технологий, однако уже есть жертвы, не только с летальным исходом разумеется, например в июле 2015 года было первое в мире ДТП с беспилотным автомобилем – сотрудники компании Google тестировали свой проект, и в результате они же и пострадали вместе с водителем автомобиля который ударился в беспилотник сзади [10].

Что же касается теоретического дистанционного угона подобного транспорта – инцидентов не было, однако заявлять о том, что это невозможно тоже не стоит, если есть возможность управления автомобилем без водителя внутри – обязательно попадутся взломщики, которые найдут способ запустить его снаружи и отправить в путь, а последствия от такого могут быть самыми разными.

Однако уже был случай, который описал журналист издания Wired [11]. Два американских специалиста по защите информации, Крис Валасек и Чарли Миллер, в 2015 году взломали дистанционно, с помощью ноутбука и смартфона на расстоянии 16 километров, автомобиль Jeep Cherokee, и что характерно: автомобиль был на ходу, а сам журналист был в машине. Взломщики умудрились остановить автомобиль на ходу на скорости 110 км/ч через лазейку информационно-развлекательной системе UConnect. В дальнейшем Chrysler (компания-производитель) отозвала 1.4 миллиона автомобилей с целью устранить данную уязвимость.

Результаты

Казалось бы, транспортные средства и киберпреступность имеют довольно слабую связь, однако чем ближе мы к внедрению беспилотных автомобилей и прогресса индустрии электромобилей – тем сильнее эта связь будет проявляться.

Как видно из предоставленных материалов – дистанционный угон транспортного средства с беспилотной системой вполне возможен, дело времени пока взломщики начнут этим заниматься, пока что проблемы не видно, но это не потому что она невозможна, а потому что беспилотные автомобили сами по себе редкость.

Однако прогресс неизбежен, как упоминалось в книге аналитиков, беспилотное будущее вполне возможно, и в этом случае правоохранительным органам необходимо уметь противостоять данным видам преступлений.

Возможно, в будущем мы столкнёмся с тем, что пока видим лишь в произведениях культуры жанра научной фантастики. Однако уже сейчас необходимо заниматься подготовкой правовой базы для подобного рода преступлений.

Например, в случае если беспилотный автомобиль собьёт человека, как это уже произошло в указанном выше случае, кто в таком случае будет считаться виноватым? Водитель или компания-разработчик программного обеспечения? Такие вопросы необходимо прорабатывать.

К слову, сравнительно недавно (на момент написания данной работы) Еврокомиссия поддержала законопроект о регулировании искусственного интеллекта [12] (в основном речь идёт о нашумевших нейросетях), который подразумевает собой обязанность компаний маркировать продукты, сгенерированные искусственным интеллектом, а также оценивать риски. Подобные законопроекты необходимы, поскольку будущее становится всё ближе.

В России на данный момент подобного закона о регулировании искусственного интеллекта нет, однако имеет место Федеральный закон "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных" от 24.04.2020 N 123-ФЗ[1],[13] но он носит скорее, как уже упоминалось, экспериментальный характер и действует лишь в одном субъекте.

Обсуждение

Теоретическая связь киберпреступности и транспортных средств видится лишь как одна из возможных проблем будущего, ведь на данный момент всё ещё многие люди пользуются автомобилями с довольно ограниченными цифровыми возможностями, а новейшие электромобили как например те же Tesla являются чем-то экзотическим. Например, по данным аналитического агентства «Автостат» самой популярной машиной в России оказалась Lada Granta [14], количества проданных которой оказалось 44059 штук в период с января по март 2023 года, к слову ближайший конкурент в данной

---

[1] Закон Российской Федерации «Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» « от 24.04.2020 № 128-ФЗ // Российская газета. – 2020

инфографике – LADA Niva Travel был продан лишь в 10449 экземплярах. Ни одна из данных моделей функцией автопилота, разумеется, не обладает, а мультимедийные системы ограничены довольно скромным набором функций.

Однако попросту игнорировать приближающееся будущее тоже нельзя, последствия этого могут быть крайне плачевны.

Выводы

Несмотря на то, что тема данной работы относится к событиям будущего, чего-то, что сейчас или отсутствует в целом, или присутствует в крайне ограниченном проявлении, начинать превентивные меры по регулированию необходимо уже сейчас.

В примере выше был упомянут законопроект Еврокомиссии по искусственному интеллекту, подобные необходимо принимать и у нас, в России. Вкупе с изменениями в действующих правилах дорожного движения и общей регулировке вопроса появления беспилотных автомобилей позволит избежать многих неприятных событий. Разумеется, вопрос относительно эффективности, безопасности, удобства использования и иные технические вопросы – прерогатива технических компаний которые занимаются разработкой подобных технологий, однако отсутствие под этим объективной и конкретной правовой базы может привести к хаосу на дорогах, человеческим жертвам, утечкам конфиденциальной информации и техническому отставанию.

Литература

1. Wakefield E.H. History of the Electric Automobile: Battery-Only Powered Cars. – Warrendale: Society of Automotive Engineers, 1993. – 572 с.
2. Ежегодник Большой Советской Энциклопедии. – М., под редакцией Ковалёва С.М.: Советская энциклопедия, 1978. – 640 с.
3. Щетина В.А., Морговский Ю.Я. Электромобиль : Техника и экономика. – Ленинград.: Машиностроение : Ленингр. отд-ние, 1987. – 252 с.
4. James A., Tony S. Rethinking Transportation 2020-2030: The Disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries. – 2017. – 162 с.
5. Данные, которые мы не уберегли, и уроки, которые мы извлекли // Яндекс блог URL: https://yandex.ru/blog/company/dannye-kotorye-my-ne-uberegli-i-uroki-kotorye-my-izvlekli (дата обращения: 12.05.2023).
6. Сбивший женщину в США беспилотный автомобиль Uber не «узнал» в ней пешехода // РИА новости URL: https://ria.ru/20191106/1560639919.html (дата обращения: 12.05.2023).
7. Project Summary: Highway Investigation – 44 Docket Items – HWY18MH010 // NTSB: National Transporttion Safety Board URL: https://data.ntsb.gov/Docket?ProjectID=96894 (дата обращения: 12.05.2023).
8. Самоуправляемая машина Google впервые попала в аварию с пострадавшими // РБК URL: https://www.rbc.ru/rbcfreenews/55a8b83b9a7947124086991c (дата обращения: 12.05.2023).

9. Hackers Remotely Kill a Jeep on the Highway—With Me in It // Wired URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (дата обращения: 13.05.2023).

10. AI Act: a step closer to the first rules on Artificial Intelligence // European Parliament News URL: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence (дата обращения: 13.05.2023).

11. Лидеры и аутсайдеры российского авторынка в 1 квартале 2023 года // Автостат: Аналитическое агентство URL: https://www.autostat.ru/infographics/54346/ (дата обращения: 13.05.2023).

Научное издание

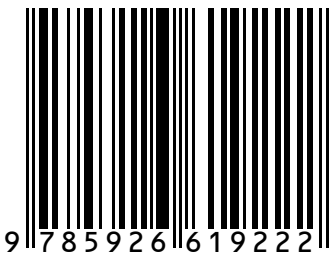
ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
Всероссийской научно-практической конференции

(18 мая 2023 г.)

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1922-2



Подписано в печать 19.07.2023.
Авт. л. 7,1. Заказ 167.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.