Федеральное государственное казенное образовательное учреждение высшего образования «Уральский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

Противодействие мошенничеству с использованием электронных средств платежа

Учебно-практическое пособие

Екатеринбург
2022

ББК 67.408.121.12
П833

П833 **Противодействие мошенничеству с использованием электронных средств платежа:** ***учебно-практическое пособие*** **/** *под ред. Н. В. Голубых*. – Екатеринбург: Уральский юридический институт МВД России, 2022. – 64 с.

ISBN 978-5-88437-907-7

Коллектив авторов

Н. В. Голубых, кандидат юридических наук, доцент (введение, глава 1 (в соавт.), общая редакция);

К. В. Потанин (глава 1 (в соавт.), заключение);

Д.Н. Лахтиков, кандидат юридических наук, доцент (глава 2 (в соавт.);

П. Л. Боровик, кандидат юридических наук, доцент (глава 2 (в соавт.)

Рецензенты: **В. В. Бабурин,** профессор кафедры криминологии и профилактики преступлений Омской академии МВД России, доктор юридических наук, профессор;

О. В. Ермакова, доцент кафедры уголовного права и криминологии Барнаульского юридического института МВД России, кандидат юридических наук, доцент

В учебно-практическом пособии на основе анализа теоретических положений, сложившейся судебной практики приведена криминологическая характеристика мошенничества с использованием электронных средств платежа и выработаны меры противодействия рассматриваемому виду мошеннических действий.

Пособие предназначено для обучающихся и преподавателей образовательных организаций МВД России, сотрудников территориальных органов внутренних дел

Обсуждено на заседании кафедры криминологии и уголовно-исполнительного права УрЮИ МВД России (протокол № 21 от 2 ноября 2022 г.).

Рекомендовано для использования в образовательном процессе методическим советом УрЮИ МВД России (протокол № 6 от 12 декабря 2022 г.).

ISBN 978-5-88437-907-7

67.408.121.12

Введение

Мошенничество как форма преступной деятельности несет в себе большую историю становления. Отправной точкой для начала развития мошенничества стало развитие торговых отношений. Так, с целью получения выгоды либо избегания своих затрат один из субъектов таких отношений, именуемый мошенником, совершал обманные действия в отношении другого субъекта рынка. В процессе развития рыночных отношений происходило увеличение как количества, так и качества мошеннических действий.

Безусловно, государственная власть принимала законодательные акты, предусматривающие меры ответственности за совершение мошенничества. Данный факт показывает, что государство признает распространенность и общественную опасность такого рода противоправных действий. При этом, наряду с законодательным закреплением ответственности за мошенничество, преступное сообщество создавало все новые способы совершения обманных действий.

Значимость разработки мер предупреждения и борьбы с изучаемым явлением с каждым годом подтверждается разработкой законодательных актов отдельных государств, принятием межгосударственных соглашений о сотрудничестве в области мошенничества, связанного с использованием информационно-телекоммуникационных технологий, в состав которых входят и электронные средства платежа. На сегодняшний момент развитие мировой экономики сопровождается повсеместным использованием информационно-телекоммуникационных технологий, в том числе электронных средств платежа. В связи с этим происходит стремительное обращение наличных средств платежа к безналичным, что стало причиной увеличения преступной активности в рамках использования электронных средств платежа как средства оплаты товаров и услуг.

На основании вышесказанного следует сказать, что в современный период времени уголовно-правовая охрана правомерного использования электронных средств платежа представляет собой значимое направление деятельности правоохранительных органов. Следовательно, актуальность проблемы предупреждения и противодействия мошенничеству с использованием электронных средств платежа не подвергается сомнению, поскольку противоправная деятельность мошенников вызывает значительную общественную опасность для общества.

Учебно-практическое пособие будет способствовать освоению тем учебных дисциплин «Криминология», «Предупреждение преступлений и административных правонарушений органов внутренних дел» и предназначено для курсантов и слушателей образовательных организаций высшего образования МВД России, обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность; по направлениям подготовки 40.03.01 Юриспруденция, 40.03.02 Обеспечение законности и правопорядка.

Теоретическая и практическая работа с материалом учебно-практического пособия поспособствует формированию у обучающихся следующих компетенций:

– способность выявлять причины и условия, способствующие совершению преступлений и иных правонарушений, предлагать меры по их предупреждению;

– способность осуществлять профилактическую деятельность среди лиц, потерпевших от преступных посягательств, в целях изменения их виктимного поведения;

– способность решать задачи профессиональной служебной деятельности по противодействию преступлениям и иным правонарушениям, в том числе совершаемым с использованием информационно-телекоммуникационных технологий и средств массовой информации.

Глава 1. Криминологическая характеристика мошенничества с использованием электронных средств платежа

Одной из неотъемлемых тенденций формирования современного информационного общества выступает повсеместная экспансия электронных денежных средств, циркулирующих с помощью специальных электронных устройств, интегрированных в платежные системы.

За последние годы платежная индустрия России добилась впечатляющих результатов, что имеет большое значение для дальнейшего становления государства.

Несмотря на стабильный рост объемов электронных платежей, который сопутствует общему развитию российской экономики, сохраняется и целый ряд проблем, таких как ограниченный опыт обращения к банковским услугам у значительной части населения, внушительный объем «серого» рынка и общая ориентация экономики на использование наличных денежных средств. Как показывает практика, электронные системы платежей способствуют стимулированию потребительских расходов.

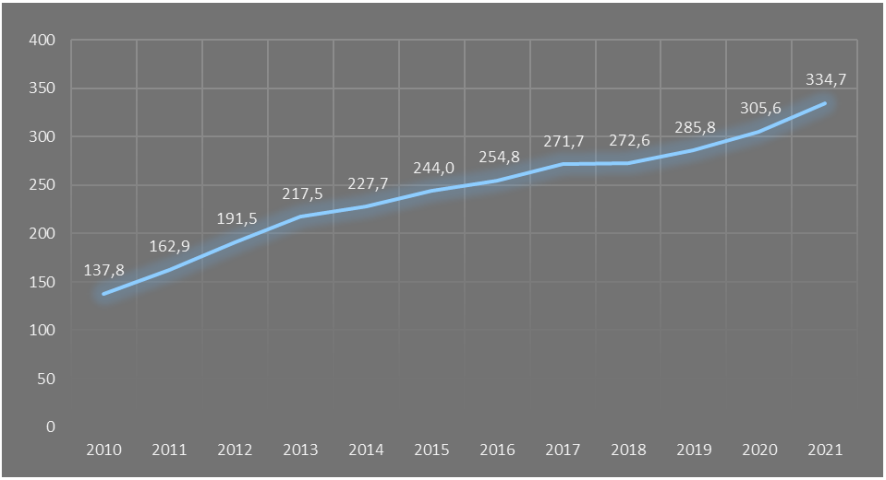

Рис. 1. Количество платежных карт, полученных на территории Российской Федерации (https://www.cbr.ru/statistics/nps/psrf)

За период с 2010 по 2021 г. количество платежных карт возросло более чем в 2 раза, что свидетельствует о качественном преобразовании в области оплаты товаров и услуг. Указанный факт отражает вытеснение некогда привычных, сложившихся столетиями товарно-денежных отношений с наличными денежными знаками, вследствие удобного, мгновенного и дистанционного характера совершения операций[1].

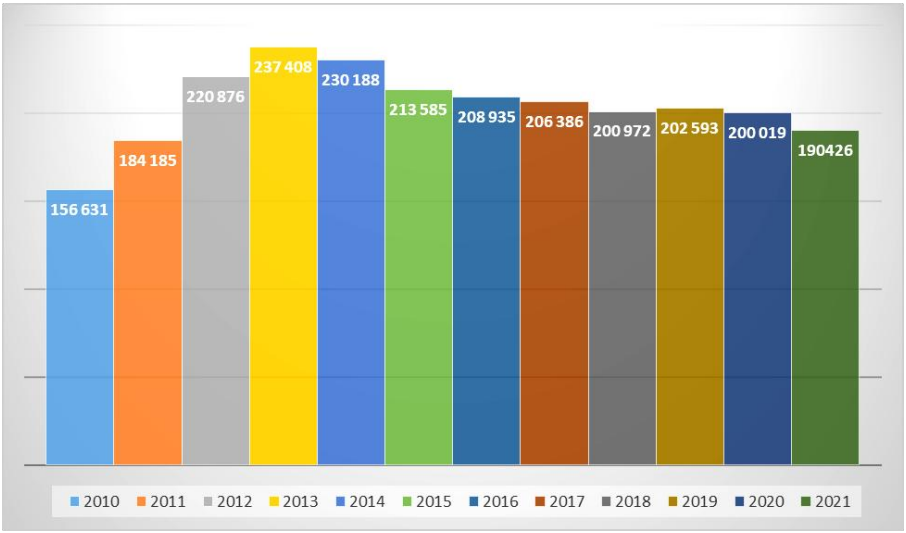

Рис. 2. Сведения об устройствах, расположенных на территории России и предназначенных для осуществления операций с использованием и без использования платежных карт (https://www.cbr.ru/statistics/nps/psrf)

С ростом числа платежных инструментов, а именно платежных карт, становился рост и устройств, предназначенных для осуществления операций с их использованием. Так в 2011 г. наблюдается минимальное количество устройств. При этом в последующие несколько лет рост таких устройств имел высокий темп, вплоть до конца 2013 г. В дальнейшем наблюдается постепенное снижение количества рассматриваемых устройств, что обуславливается уточнением ряда круп-

[1] Данные судебной статистики // Судебный Департамент при Верховном Суде Российской Федерации: официальный сайт. URL: http://www.cdep.ru/index.php?id=79.

ных кредитных организаций методики внутреннего учета данного показателя, а также в связи с переквалификацией типов устройств.

С целью регулирования постепенного перехода участников торгово-хозяйственных отношений для обслуживания в электронную систему платежа законодателем 27 июня 2011 г. был принят Федеральный закон № 161-ФЗ «О национальной платежной системе». Предметом данного закона, в соответствии со ст. 1, является установление правовых и организационных основ национальной платежной системы, регулирование порядка оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, деятельности субъектов национальной платежной системы, а также определение требований к организации и функционированию платежных систем, порядка осуществления надзора и наблюдения в национальной платежной системе[1].

В ст. 3 указанного нормативного акта приводится определение термина «электронные средства платежа», под которым понимается средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

[1] О национальной платежной системе: федеральный закон Российской Федерации от 27 июня 2011 года № 161-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru.

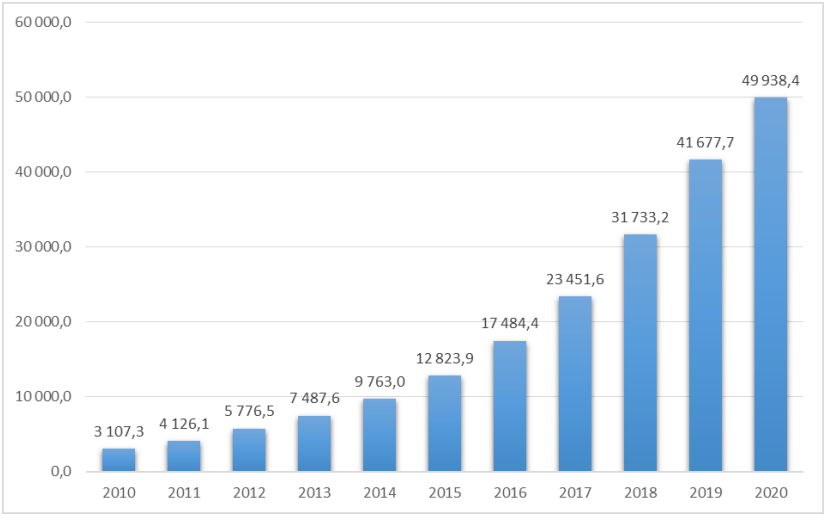

Рис. 3. Операции, совершенные на территории России с использованием карт, эмитированных российскими кредитными организациями (млн ед.) (https://www.cbr.ru/statistics/nps/psrf)

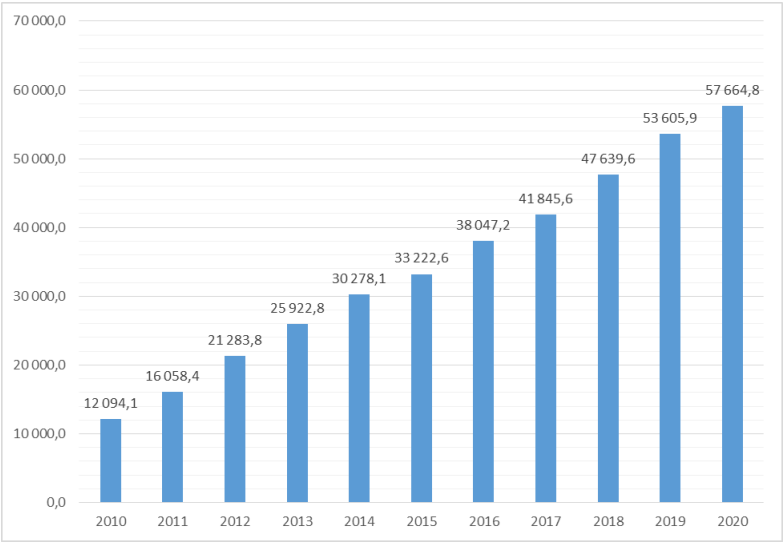

Рис. 4. Объем денежных средств в платежных операциях с использованием платежных карт (млрд руб.) (https://www.cbr.ru/statistics/nps/psrf)

Электронные платежные системы и платежные терминалы стали привычным атрибутом повседневной жизни россиян. По мере роста количества платежных карт возрастает и количество операций, и сумм безналичных операций, что привело к увеличению количества противоправных деяний в отношении владельцев денежных средств.

Тем самым увеличение использования электронных средств платежа напрямую соотносится с ростом преступлений с их использованием, что можно отнести к основной группе детерминантов рассматриваемого вида преступлений.

Преступления, совершаемые в сфере проведения безналичных расчетов с использованием банковских карт, относятся к качественно новому виду корыстной преступности в банковской сфере, которая непосредственно связана с модернизацией экономических отношений в обществе. В связи с этим изучаемая группа преступлений, получивших в статистических материалах название «преступления экономической направленности», может посягать как на собственность и другие экономические интересы государства, отдельных групп граждан (потребителей, партнеров, конкурентов), так и на порядок управления экономической деятельностью в целях извлечения наживы.

В России уголовная ответственность за мошенничество с использованием электронных средств платежа была установлена в ноябре 2012 г. Изначально ст. 159.3 УК РФ получила название «Мошенничество с использованием платежных карт», но в апреле 2018 г. законодатель внес в рассматриваемую норму корректировки, расширив сферу ее применения. В данный момент мошеннические действия, совершенные как с использованием платежных карт, так и при эксплуатации инструментов интернет-банкинга, электронных кошельков и других платежных сервисов, популярных среди населения, могут квалифицироваться по ст. 159.3 УК РФ.

С 2012 года по настоящее время доля мошенничеств, предусмотренных ст. 159–159.6 УК РФ, в составе всей совокупности преступлений с каждым годом занимала значительную часть:

2012 год – общее количество зарегистрированных преступлений было 2 302 168, из них 161 696 – мошенничеств, что составляет 7,0 %;

2013 год – общее количество зарегистрированных преступлений – 2 206 249, из них 164 629 – мошенничеств – 7,5 %;

2014 год – общее количество зарегистрированных преступлений – 2 190 578, из них 160 214 – мошенничеств – 7,3 %;

2015 год – общее количество зарегистрированных преступлений – 2 388 476, из них 200 598 – мошенничеств – 8,4 %;

2016 год – общее количество зарегистрированных преступлений – 2 160 063, из них 208 962 – мошенничеств – 9,7 %;

2017 год – общее количество зарегистрированных преступлений – 2058476, из них 222772 – мошенничеств – 10,8 %;

2018 год – общее количество зарегистрированных преступлений – 1 991 532, из них 215 036 – мошенничеств – 10,8 %;

2019 год – общее количество зарегистрированных преступлений – 2 024 337, из них 257 187 – мошенничеств – 12,7 %;

2020 год – общее количество зарегистрированных преступлений – 2 044 221, из них 335 631 – мошенничеств – 16,4 %

2021 год – общее количество зарегистрированных преступлений – 2 004 404, из них 339 606 – мошенничеств – 16,9 %[1].

В Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» дано разъяснение по уголовно-правовым составам ст. 159.1–159.6 УК РФ. Так, в нем определено, что данные составы необходимо понимать как специальные разновидности общего состава мошенничества, закрепленного в ст. 159 УК РФ «Мошенничество».

В этой связи можно сделать вывод, что юридическая модель ст. 159 УК РФ является основой (родовой частью), а производные от нее «новые» составы – видовыми уголовно-правовыми конструкциями (составляющими). При этом родовая и видовые части в совокупности направлены на создание широкого юридического поля для противодействия мошенничеству, совершаемому в различных сферах деятельности и различными способами. Таким образом, ст. 159.3 УК РФ по составу преступления является «специальным» видом мошенничества и в то же время одним из видов или / и самостоятельных форм хищения.

В 2020 году было осуждено 3084 человека по следующим частям рассматриваемой нормы уголовного закона:

– ч.1 ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа) – 1243 человека (40,3 %);

[1] Состояние преступности // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://мвд.рф/folder/101762.

– ч. 2 ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа, совершенное группой лиц по предварительному сговору, а ровно с причинением значительного ущерба гражданину) – 1825 человек (59,2 %);

– ч. 3 ст. 159.3 УК РФ (деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а ровно в крупном размере) – 13 человек (0,4 %);

– ч. 4 ст. 159.3 УК РФ (деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере) – 3 человека (0,1 %)[1].

Особую общественную опасность представляют мошеннические действия, отличающиеся от других имущественных преступлений тем, что потерпевший добровольно отдает свое имущество преступнику вследствие обмана или злоупотребления доверием, которые вводят жертву в заблуждение[2]. Социальная инженерия представляет собой атаку не на сервер и не на компьютер банка, а на сознание его клиента. Например, преступникам необходимо получить пароль, для чего они высылают письмо от имени сервиса, который сходен с официальным, с уведомлением о том, что с аккаунта клиента был осуществлен несанкционированный вход, в связи с чем предлагается указать старый пароль для замены на новый. Возможны и другие варианты, такие как: исследование информации, содержащейся в социальных сетях, общение в чате, предложения заполнения анкет в целях выявления ответа на секретный вопрос клиента банка, необходимый для замены пароля.

Используя методы социальной инженерии, основанные на достижениях современных информационных технологий, мошенники выманивают у пользователей необходимые для осуществления незаконных платежей или переводов реквизиты (например, сеансовые пароли, используемые для подтверждения клиентом согласия на совершение операций с помощью мобильных приложений, пароли защищенного

[1] Состояние преступности // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://мвд.рф/folder/101762.

[2] 4 мая 2018 г. вступили в силу изменения в ст. 159.3 Уголовного кодекса Российской Федерации (Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в УК Российской Федерации»). Прежняя редакция этой статьи предусматривала ответственность исключительно за мошенничество с использованием платежных карт, в то время как ее действующая редакция предусматривает ответственность за мошенничество с использованием ЭСП.

протокола авторизации «3-D Secure») либо осуществляют несанкционированный доступ к пользовательской информации, позволяющей выполнить авторизацию и последующее хищение денежных средств со счетов пользователей.

Необходимость использования сведений о личности субъектов преступлений возникает при криминологическом анализе любого вида преступности, исследовании ее причин, при научной разработке и обосновании организации борьбы с преступностью и по предупреждению преступлений, образующих соответствующий вид преступности.

Социально-экономическое положение и внутренние качества лиц, совершающих мошенничество с использованием электронных средств платежа, зачастую подталкивает их на совершение указанных преступлений.

К личностным качествам можно отнести корысть, жажду наживы, чувство легкодоступности чужого имущества, а именно денежных средств, доступ к которым возможен с использованием сети «Интернет» и чувство безнаказанности ввиду возникающих сложностей в процессе расследования такого вида преступлений.

К социально-экономическому положению, на наш взгляд, относятся следующие факторы: несовершенство законодательства, уровень инфляции, доступность и качество образования, низкий уровень заработной платы.

Осужденные по ст. 159.3 УК РФ по уровню образования разделены на 4 группы, среди которых лица, получившие среднее профессиональное образование, составляют 40,6 % (1253 чел.), среднее общее – 36,8 % (1134 чел.), основное общее, начальное либо без образования – 19,3 % (594 чел.), высшее образование – 3,3 % (103 чел.)[1].

[1] Состояние преступности // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://мвд.рф/folder/101762.

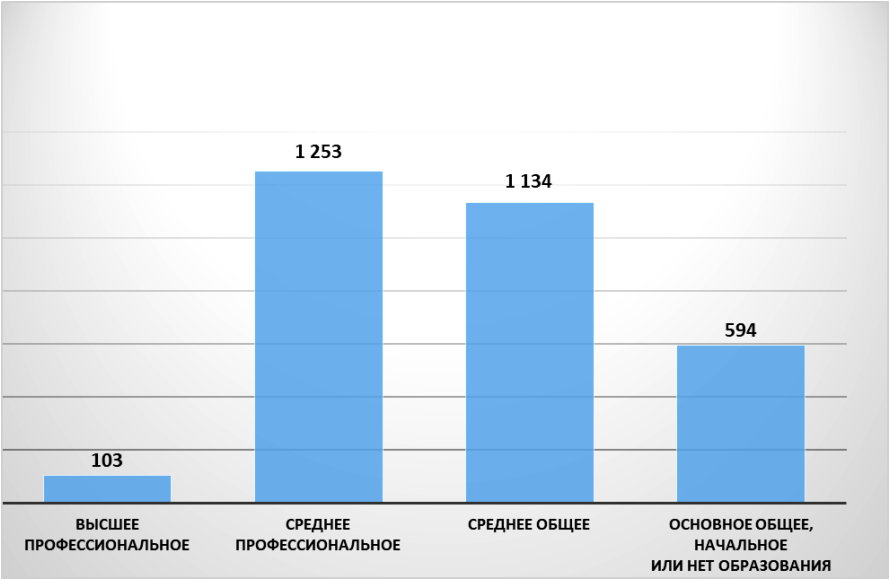

Рис. 5. Уровень образования лиц, осужденных по ст.159.3 УК РФ

Зачастую уровень заработка лиц, получивших высшее образование, позволяет им получать достаточный доход для обеспечения своих потребностей, в отличие от остальных категорий граждан, что, в свою очередь, и подталкивает последних на совершение преступлений.

На уровень заработка гражданина также влияет: место его работы, как произошло трудоустройство (официально или неофициально), зарегистрирован ли он в качестве юридического лица, индивидуального предпринимателя, самозанятого либо работает по найму. Обращаясь к статистическим данным осужденных, можно отметить, что основная часть является трудоспособной, однако не имеет постоянного источника дохода – 2217 человек, что составляет 71,9 % от общего количества за рассматриваемый период[1].

Анализ возраста осужденных показывает уровень предрасположенности к совершению мошенничеств с использованием электронных средств платежа и поможет в определении направлений профилактической работы, касающейся конкретной возрастной группы.

[1] Данные судебной статистики // Судебный Департамент при Верховном Суде Российской Федерации: официальный сайт. URL: http://www.cdep.ru/index.php?id=79.

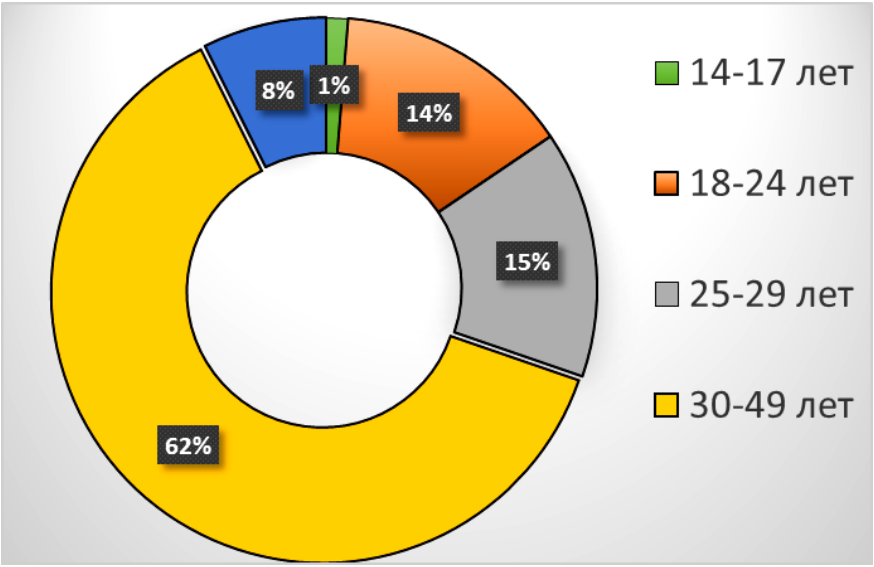

Рис. 6. Возраст осужденных лиц на момент совершения преступления

Одним из ключевых источников информации о преступном поведении лица, совершившего общественно опасное деяние, является способ преступления – совокупность используемых при его совершении приемов и методов, последовательность совершаемых преступных действий, применения средств воздействия на предмет посягательства. Способ указывает, какие именно действия произведены, выражает субъективные компоненты личности преступника, форму его вины, мотив и цели, характер применяемых орудий и средства[1]. Это предопределяет криминологическую сущность способов мошенничества с использованием ЭСП и обосновывает практическую значимость их рассмотрения.

Основными тенденциями совершаемых хищений в рассматриваемой сфере[2] являются:

[1] См.: *Зуйков Г. Г.* Криминалистическое учение о способе совершения преступления: автореф. дис. ... д-ра юрид. наук. М., 1970. С. 19.

[2] По данным ОАО «Банковский процессинговый центр» (специализированный центр по информационно-технологическому обеспечению безналичных расчетов с использованием

- увеличение количества мошенничеств с использованием социальной инженерии (фишинг, вишинг, взлом учетных записей пользователей в социальных сетях);
- звонки в результате утечки персональных данных, например, на маркетплейсе «Joom»;
- наличие фактов компрометации системы ДБО клиентов в рамках социальной инженерии, в результате чего преступники получают учетные данные (логины, пароли и ключи) доступа к системе ДБО;
- мошенничество по токенам, когда преступники с использованием социальной инженерии выманивают не только реквизиты платежной карты и «3-D Secure» пароль, но и данные, необходимые для присвоения токена к платежной карте, привязывают токен держателя на свое мобильное устройство. В настоящее время «3-D Secure» является самым распространенным методом дополнительной проверки;
- рассылка в социальных сетях уведомлений о выигрышах, когда держатели сами вводят реквизиты платежных карт для получения выигрыша;
- увеличение количества мошеннических операций на онлайн-сервисах, которые занимаются продажей цифровых товаров: компьютерных игр и программного обеспечения (взлом аккаунтов учетной записи Google, после осуществляются операции оплаты Google сервисов в пределах остатка баланса на счете);
- увеличение количества мошеннических тестовых операций и атак на БИНы банков (сгенерированные номера платежных карт) на сайтах, зарегистрированных на территории США, Индии и Бразилии;
- присутствие фактов «friendlyfraud» мошенничества. Например, когда злоумышленником в интернет-магазине заказывается и оплачивается товар, а затем происходит убеждение продавца совершить возврат денежных средств, мотивируя тем, что произошло хищение банковской платежной карты, взлом электронного кошелька или используется другой повод с целью возмещения денежных средств, при этом предпринимается попытка оставить товар;
- вещевой кардинг;

банковских платежных карт отечественной платежной системы и международных систем, действующих на территории Республики Беларусь).

- смещение мошенничества с использованием электронных платежных инструментов и сервисов все больше в сферу электронной коммерции.

Также специалистами отмечается, что в ближайшей перспективе будут актуальны следующие способы мошенничества:

- с использованием социальной инженерии, что будет актуально до повышения уровня финансовой цифровой грамотности пользователей;
- перехват доступа к интернет-банкингу, что предоставляет преступнику получение доступа ко всем платежным картам и счетам, появляется возможность открывать кредитные линии;
- использование шифровальщиков, когда трояны-вымогатели, блокируют доступ к данным и требуют определенную сумму для возвращения доступа к информации;
- использование банковских «троянов»;
- компрометация межбанковской системы идентификации;
- атаки на сотрудников, работающих удаленно, поскольку преодоление систем защиты вне корпоративной сети осуществляется легче;
- более активное использование искусственного интеллекта, например, для создания дипфейков, повышения эффективности вредоносного программного обеспечения, преодоление защиты «captcha», подбора паролей, анализа больших массивов данных с целью извлечения номеров телефонов и реквизитов платежных карт.

В свою очередь, в Российской Федерации и в Республике Беларусь функционируют ФинЦерты, т. е. центры мониторинга и реагирования на угрозы информационной безопасности в банковской сфере, которые осуществляют выявление и нейтрализацию киберугроз и оперативный обмен информацией между заинтересованными субъектами с целью их предупреждения или минимизации последствий.

Анализируя правоприменительную практику по делам о совершении мошенничеств с использованием ЭСП, следует отметить, что в преобладающем большинстве случаев в банковских и иных финансовых организациях, клиенты которых пострадали от мошеннических действий злоумышленников, были созданы определенные организационные и технические условия обеспечения информационной безопасности. Однако важно понимать, что этот процесс не статичен и

требует постоянного совершенствования средств, методов и технологий защиты на всех участках информационного контура, который формируется в процессе выполнения расчетов между участниками сделки. Специалистами справедливо подчеркивается, что помимо регламентации внутренних процедур должны быть предусмотрены современные технические средства информационной безопасности, которые помогут предотвращать случаи хищения денежных средств с помощью систем разграничения доступа, мониторинга совершенных пользователем операций, реагирования на инциденты[1].

Подводя промежуточный итог, следует отметить, что широкое применение таких новых форм безналичных расчетов, как расчеты с использованием различных электронных средств платежа, а также использование возможностей последних достижений научно-технического прогресса на фоне ненадлежащего правового регулирования деятельности в банковской сфере привело к значительному росту преступлений в указанной сфере.

Совершаемые в этой сфере криминальные посягательства относятся к качественно новому виду корыстной преступности и отличаются большим разнообразием способов их совершения, особой изощренностью, высокоинтеллектуальным характером, активной адаптацией преступников к новым формам и методам хозяйственной деятельности, применяемым к новым электронным платежным средствам и средствам связи.

Криминогенность сферы безналичных расчетов обусловлена как социально-экономическими, организационными, так и иными объективными и субъективными факторами, к числу которых необходимо отнести возможность быстрого и неконтролируемого использования платежных систем, несовершенство правового регулирования, отсутствие эффективных средств охраны, обеспечивающих полную безопасность банковских карт, и низкий уровень заработной платы населения.

[1] См.: *Денисов Д.* Актуальные вопросы противодействия мошенничеству в области электронных платежей // Банковский Вестник. № 1. 2014. С. 61–64.

Вопросы для самоконтроля

1. Используя данные правовой статистики, определите динамику мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий, за последние три года.

2. Охарактеризуйте личность преступника, совершающего мошенничество с использованием электронных средств платежа.

3. Перечислите наиболее распространенные способы совершения мошенничества с использованием электронных средств платежа.

4. В городе N с населением 20 тыс. человек было за год совершено 150 мошенничеств с использованием электронных средств платежа, в городе М с населением 1 млн человек было за год совершено 1 тыс. таких преступлений. Определите коэффициент мошенничеств с использованием электронных средств платежа для каждого из населенных пунктов, сравните получившиеся коэффициенты.

Глава 2. Меры противодействия мошенничеству с использованием электронных средств платежа

Современное состояние развития общества и экономики характеризуется существенным увеличением доли безналичного денежного оборота в общем объеме финансовых транзакций, что обусловлено активным внедрением различных систем расчетов с использованием электронных средств платежа[1]. К ним относится широкий перечень средств оплаты товаров и услуг или денежных переводов: платежные карты, мобильные устройства и персональные компьютеры с доступом к банковским счетам и аккаунтам, электронные платежные системы и системы дистанционного банковского обслуживания «Клиент-банк».

Разнообразие способов мошенничества с использованием ЭСП диктует необходимость их тщательного изучения с целью выработки научно-обоснованных рекомендаций по противодействию. При этом в контексте растущей общественной опасности данных преступлений особое значение приобретают технические (программно-технические) меры противодействия, что обуславливает актуальность данной проблемы.

Впервые на монографическом уровне проблема противодействия мошенничеству с использованием ЭСП была затронута авторским коллективом под общей редакцией Л. В. Лямина (2016 г.)[2]. Специалистами исследованы различные аспекты информационной безопасности, представлены подходы и методы борьбы с преступностью в платежной сфере. Работа является результатом одного из первых опытов обобщения теории и практики противодействия уголовно-наказуемым деяниям данной категории и, без сомнения, заслуживает определенного внимания. Вместе с тем стремительное развитие цифровых технологий, разнообразие существующих ЭСП, появление новых видов и

[1] Здесь и далее под электронным средством платежа понимается средство и / или способ, которые позволяют клиенту оператора по переводу денежных средств составлять / удостоверять / передавать распоряжения для перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации (в том числе платежных карт), а также других технических устройств.

[2] См.: *Лямин Л., Пятиизбянцев Н., Пухов А.* Мошенничество в платежной сфере: Бизнес-энциклопедия. М.: ЦИПСиР, 2016. С. 215.

способов мошенничества требуют дальнейшего предметного и комплексного изучения обозначенной проблемы.

Отдельные вопросы рассматриваемой проблематики затрагивались также в работах Р. Н. Боровского, Г. Н. Доронина, Л. М. Прозументова, А. В. Шеслера, А. И. Долгова, В. Н. Кудрявцева, В. Е. Эминова, С. Л. Алексеева, Я. И. Гилинского, Б. Э. Шавалеева (2013–2020 гг.) и др. Представляя собой «срез» текущего положения дел в части, касающейся программно-технических аспектов противодействия преступности обозначенного вида, исследования указанных авторов не претендуют на окончательность и однозначность содержащихся в них теоретических положений, выводов и практических рекомендаций.

Значимым научно-практическим событием, посвященным рассматриваемой проблематике, стало проведение в Республике Беларусь семинара «Расследование инцидентов информационной безопасности в системах электронных платежей» (2013 г.). На нем эксперты из России и Беларуси впервые затронули круг проблем в сфере противодействия преступности в финансовой сфере, предприняли попытку представить банковским и иным финансовым организациями методы и средства их решения[1]. Несмотря на высокую научную и практическую значимость этого мероприятия, современные программно-технические подходы к противодействию преступности данной категории остались рассмотренными фрагментарно.

Наиболее распространенными инструментами электронных средств платежа являются технологии онлайн-платежей на основе банковских платежных карт, электронных денег, интернет-банкинга (система ДБО).

Обращение электронных денег осуществляется в сети «Интернет», их можно использовать при помощи электронных (виртуальных кошельков), интернет-банкинга, устройств, работающих с банковскими платежными картами и др. Интернет-банкинг является технологией ДБО, позволяющей осуществлять управление счетами с использованием компьютерной сети «Интернет», а также предоставлять посредством программно-аппаратных средств и компьютерной сети «Интернет» банковские услуги. Получение доступа к системе ДБО возможно посредством портативного устройства и персонального компьютера с

[1] Денисов Д. Указ. соч. С. 61–64.

использованием специального приложения (программного обеспечения) или браузера (web-клиента).

При совершении указанного вида преступлений злоумышленники досконально изучают особенности функционирования ЭСП, в том числе программно-техническое обеспечение, с целью использования различных технологических особенностей в преступных целях, устанавливают уязвимости, которые используют при совершении хищений. После чего возможна разработка соответствующего программного обеспечения либо его приобретение на специализированных Интернет-ресурсах, в том числе в Даркнете. Эксплуатируя выявленную уязвимость или технологическую особенность похищаются денежные средства и перемещаются на счета, контролируемые преступниками (например, используются дропы и др.), после чего осуществляется их вывод с указанного счета и обналичивание.

Основными участниками технологии онлайн-платежей могут являться: покупатель (владелец счета, электронных денег и т. п.); продавец (например, интернет-магазин, предприятие торговли (услуг), платежная система, платежный агрегатор, платежный шлюз, эмиссионный банк, банк-эквайер, процессинговый центр.

Например, совершая платеж, покупатель вводит платежные данные через веб-интерфейс сайта интернет-магазина, после чего информация передается через платежный шлюз в банк-эквайер, который отправляет запрос на платеж в платежную систему, получает запрос на авторизацию, отправляет этот код назад в платежную систему, которая совершает операцию, код авторизации возвращается в платежный шлюз, а также этот же код уходит в интернет-магазин с результатом операции.

Для использования ЭСП на компьютер или мобильный телефон может устанавливаться специально предназначенное для этого программное обеспечение, которое поддерживает ведение локально или удаленно электронного (виртуального кошелька), который можно пополнить денежными средствами (например, банковский, почтовый перевод), а также за счет перечисления из других кошельков. Электронный (виртуальный) кошелек – это специальное программное обеспечение, которое необходимо для учета и управления электронной наличностью и, как правило, представляет собой сложный код, отражающий состояние денег в системах. Электронные платежные системы являются составной частью отношений банк – клиент, и в

обобщенном виде в любых электронных расчетах за владельцами электронных платежных систем будут стоять провайдеры и банки. Следовательно, электронные платежные системы выступают, с одной стороны, как составная часть банковской системы (и тогда на них распространяется действие банковского законодательства), а с другой – как самостоятельныеи субъекты, осуществляющие расчетные операции[1].

Платежная система – это финансовая инфраструктура, обеспечивающая совершение финансовых транзакций между банками и иными участниками рынка финансовых операций.

С позиции технической составляющей, это аппаратно-программный комплекс со своей технической инфраструктурой, сводом правил и процедур, обеспечивающих бесперебойное совершение финансовых транзакций согласно международному, национальному законодательству и своим правилам.

Типичная платежная система может состоять из следующих составляющих: организации (подразделения), осуществляющие платежи; программно-аппаратное обеспечение, осуществляющее внутренние и внешние финансовые транзакции; нормативная правовая база, регламентирующая работу. Ключевой задачей платежной системы является оперативное проведение взаиморасчетов между участниками.

Можно выделить такие виды платежных систем, как: системы с участием наличных денег, безналичные платежные системы, банковские платежные карты, электронные платежные системы.

Платежная система может быть разного уровня: может работать как на уровне одной страны, так и обеспечивать интересы нескольких стран. В международных расчетах особое место занимает система международных межбанковских расчетов SWIFT (Society for Worldwide Interbank Financial Telecommunication – сообщество всемирных межбанковских финансовых телекоммуникаций), которая охватывает более 11 000 банков во всем мире. В системе SWIFT каналы, через которые проходят финансы, являются инфраструктурными решениями, которые обеспечивают передвижение денежных средств от одного субъекта к другому, например, от покупателя к продавцу. В

[1] См.: *Олиндер Н. В.* Криминалистическая характеристика электронных платежных средств и систем // LEX RUSSICA (РУССКИЙ ЗАКОН). 2015. № 10. С. 128–138.

отдельных случаях под международной платежной системой имеют ввиду только системы, обслуживающие платежные карты (типа VISA, MasterCard и др.).

В Российской Федерации и Республике Беларусь наиболее распространенными электронными платежными системами являются:

Яндекс.Деньги (один из сервисов Яндекса). После регистрации в системе создается электронный кошелек, который пополняется с использованием банковской платежной карты или наличных денег. Используется для оплаты товаров и услуг посредством компьютерной сети «Интернет», а также для совершения денежных переводов. Предоставляется возможность выпуска виртуальной карты, которой возможна оплата товаров и услуг при онлайн-платежах, где принимают к оплате банковские платежные карты.

WebMoney. Система российского происхождения, имеющая электронные аналоги российского и белорусского рубля, украинской гривны, казахстанского тенге, доллара США, евро, золота, криптовалют (биткоина, лайткоина), которая используется во многих странах СНГ. Является одним из популярных сервисов электронных кошельков. После регистрации выдается номер в системе, который называется WMID, имеется возможность создания электронных кошельков в нужной валюте, к которым возможен выпуск виртуальной карты.

PayPal. Международная мультивалютная платежная система, действующая во многих странах мира, которая используется для различных платежей. При регистрации указываются полные данные, в том числе адрес электронной почты, и открывается счет без присвоения номера, вместо него используется указанный при регистрации адрес электронной почты. Для проведения платежей необходима привязка платежной карты к счету на сайте.

Qiwi. Регистрация в системе происходит по номеру мобильного телефона, который является счетом в системе и пополняется, например, через платежный терминал банковской картой. Возможен выпуск виртуальной карты или платежной карты Visa.

В Республике Беларусь также функционирует национальная платежная система IPay-сервис, интегрированная с названными выше платежными системами, а также с ЕРИП и мобильными операторами.

Также в Республике Беларусь Национальным банком создана система провайдер «Расчет» (Единое расчетное информационное пространство), с помощью которой осуществляется поддержка при про-

ведении онлайн-платежей. ЕРИП позволяет проводить различные виды расчетов, включая коммунальные услуги, покупки в интернет-магазинах, билеты в кино и др. Возможно подключение системы ЕРИП как напрямую, так и с помощью платежных агрегаторов.

Платежный агрегатор обрабатывает онлайн-платежи. Так, например, владелец интернет-магазина либо самостоятельно организовывает прием платежей с каждой из платежных систем, либо заключает договор с платежным агрегатором, у которого имеются технические решения для работы с платежными системами.

Наиболее распространенными платежными агрегаторами в Республике Беларусь являются:

WebPay (обеспечивает комплексные решения для приема онлайн-платежей по картам Visa, MasterCard, Белкарт);

Платежный агрегатор bePaid предназначен для юридических лиц и индивидуальных предпринимателей, которые продают товары (услуги) через компьютерную сеть «Интернет». Данная система принимает оплату с помощью карт Visa, MasterCard, Белкарт, Халва. Проводит платежи в белорусских и российских рублях, а также в евро и долларах;

Агрегатор Assist может принимать к оплате банковские карты Visa, MasterCard, Maestro, AmericanExpress, Белкарт прямо на сайте;

Агрегатор EasyPay позволяет осуществлять платежи банковскими картами Visa и MasterCard, а также через систему ЕРИП.

Одними из наиболее популярных платежных агрегаторов в Российской Федерации являются Яндекс.касса, Robokassa, Z-payment и другие.

Платежный шлюз – это сервис, который осуществляет маршрутизацию платежа. С технической точки зрения платежный шлюз является программным модулем, который распределяет (осуществляет маршрутизацию) платежа между участниками транзакции: интернет-магазин, банк и третьи стороны, – вовлеченных в процесс (например, предоставляющие услуги эквайеринга).

Платежный шлюз является интегратором платежных решений, который не выполняет какой-либо расчетно-финансовой функции. Однако платежные агрегатор и шлюз осуществляют интеграцию платежных инструментов для осуществления онлайн-платежей посредством широкого набора разных опций (платежные карты, электронные кошельки, оффлайн-платежи и др.).

Отличия платежного агрегатора и платежного шлюза:

– платежный агрегатор аккумулирует денежные средства клиента у себя, что делает его полноценной небанковской кредитной организацией;

– платежный шлюз лишь маршрутизирует платеж, с денежными средствами, вовлеченными в транзакционный обмен, не взаимодействует. Другими словами, платежный шлюз исключительно выполняет роль технологического посредника;

– платежный шлюз, в отличие от платежного агрегатора, не несет ответственности за транзакцию, соответственно, не несет риски по движениям денежных средств (например, возвраты);

– платежный агрегатора аккумулирует денежные средства клиентов на своем счете, прежде чем отсылать их в банк. Из-за этого может возникать риск небольшой отсрочки платежа по отношению к банку, а также возможность создания прецедента с «заморозкой» денежных средств при технологических сбоях;

– платежные шлюзы в основном предоставляют услуги мультиэквайринга, при возникновении проблем с обработкой платежа в одном банке шлюз быстро перемаршрутизирует платеж в другой банк.

Таким образом, основное отличие заключается в том, что платежный шлюз является технологическим партнером, который маршрутизирует платеж, не взаимодействуя с денежными средствами клиентов, в то время как платежный агрегатор их аккумулирует у себя.

Банк-эквайер – кредитно-финансовая организация, обеспечивающая расчеты по банковским платежным картам в торгово-сервисных организациях. Для обработки онлайн-платежей банк-эквайер использует платежный агрегатор или платежный шлюз.

Эмиссионный банк (или кредитно-финансовая организация), осуществляющий выпуск (эмиссию) и в отдельных случаях обслуживание платежных карт, являющийся владельцем платежной карты. Основные функции банка-эмитента следующие: открытие счета, выпуск платежной карты, проведение авторизации платежей по своим платежным картам, совершение платежа в сторону продавца, если клиент совершил покупку, обеспечение безопасности транзакций.

Процессинговый центр – организация или его структурное подразделение, обеспечивающее технологическое и информационное взаимодействие между участниками расчетов.

Среди наиболее распространенных способов совершения преступлений указанного вида особой популярностью у мошенников пользуется *фишинг*. Термин образован от английского словосочетания «passwordfishing» («выуживание паролей») и в классической интерпретации означает «введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной интернет-системы, предполагающей идентификацию пользователя»[1]. Главная задача мошенника – заманить пользователя на этот сайт и убедить его сообщить идентификационные либо иные персональные данные. Для этого злоумышленники используют следующие приемы и методы[2]:

1. Рассылка спама (недобросовестная реклама товаров, которые можно приобрести в интернет-магазине, причем в рекламе обязательно приводится ссылка на сайт магазина-однодневки либо поддельный сайт, визуально неотличимый от настоящего). Осуществляется с помощью СМС-сообщений, электронной почты, рекламных баннеров на веб-сайтах, новостных лент, популярных интернет-мессенджеров (WhatsApp, Viber, Telegram, Facebook), коммуникативно-развлекательных мобильных приложений (Snapchat, TikTok) и социальных сетей (Instagram, ВКонтакте, Twitter, Tinder и др.).

Особую значимость рассматриваемый метод приобрел с распространением онлайн-сервиса «Bit.ly» (https://bitly.com), предназначенного для создания сокращенных URL-адресов. Данный сервис сокращает ссылку, превращая ее фактически в семь символов, следующих за приставкой-названием самого сервиса, например: *bit.ly/2ByeRZX*. Суть такого сокращения – сделать ссылку более компактной для рассылки, а следовательно – более кликабельной.

2. *Использование вредоносного программного обеспечения (далее – ВПО) класса «Троян»* (например, Trojan.Win32.DNSChanger), проникающих в компьютер пользователя под видом легитимного программного обеспечения (в данную категорию обычно входят программы,

[1] *Зайцев О.* Мошенничество в Интернете и защита от него // КомпьютерПресс: сайт. URL: https://compress.ru/article.aspx?id=18184.

[2] Значительная часть мошенничеств указанного вида основывается на различных методах так называемой социальной инженерии и ориентированы на обман владельцев карточных счетов. Такие способы рассматриваться нами не будут, поскольку основой их противодействия являются не программно-технические меры, а активная и последовательная разъяснительно-предупредительная работа с клиентами со стороны банковских и иных финансовых организаций. Данная специфика не является предметом нашего исследования.

выполняющие различные неподтвержденные пользователем действия: сбор информации о банковских картах и передача этой информации злоумышленнику, использование ресурсов компьютера в целях майнинга, нелегальной торговли и др.).

Упрощенной формой реализации данного метода является несанкционированная модификация файла *Hosts* (текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов; запрос к этому файлу имеет приоритет перед обращением к DNS-серверам). Более сложные методы основаны на применении ВПО класса «Руткит» (англ. rootkit, то есть «набор root-a»), обеспечивающих маскировку объектов (процессов, файлов, каталогов, драйверов), управление (событиями, происходящими в системе) и сбор данных (параметров системы).

Специфика указанных методов заключается в том, что вредоносный код может использовать авторизацию пользователя в системе для получения к ней расширенного доступа или для получения его авторизационных данных. Кроме того, вредоносный код может быть внедрен в страницу как через уязвимость на веб-сервере, так и через уязвимость на компьютере пользователя[1].

Разновидностью фишинга является преднамеренное введение пользователя в заблуждение посредством использования *программного обеспечения класса Hoax*[2] (в переводе с англ. означает «обман») с целью получения финансовой выгоды. Такие программы значительно преувеличивают эффект имеющихся проблем либо вовсе выдают на экран информацию о несуществующих ошибках в работе компьютера, вынуждая пользователя заплатить деньги за подобный функционал, чтобы избавить компьютер от якобы обнаруженных ими угроз. При этом подобные программы чаще всего именно вынуждают, а не предлагают себя приобрести, объявляя пользователю, что без оплаты проблему не решить.

В последние годы фишинговым атакам активно подвергаются клиенты не только крупных банков, но и небольших кредитных организа-

[1] См.: *Дудников Е. А.* Анализ существующих целей сетевых атак и способов атак на web-сервисы. URL: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-tseley-setevyh-atak-i-sposobov-atak-na-web-servisy.

[2] Антивирусное программное обеспечение «Лаборатории Касперского» к подобным программам относит следующие: HEUR:Hoax.Win32.Uniblue.gen, Hoax.Win32.PCFixer.gen, Hoax.Win32.DeceptPCClean.*, Hoax.Win32.PCRepair.*, HEUR:Hoax.Win32.PCRepair.gen, HEUR:Hoax.MSIL.Optimizer.gen, Hoax.Win32.SpeedUpMyPC.gen и другие.

ций. В качестве примера можно привести фишинговый сайт «Севергазбанка» (РФ) (https://severogazbank.com), предлагающий в «личном кабинете» ввести данные платежной карты и код двухфакторной аутентификации из СМС-сообщения (рис. 7). Подобные фишинговые сайты появляются ежедневно, а слово «банк» остается одним из самых популярных слов в составе доменных имен (рис. 7).

Помимо фейковых личных кабинетов существующих банков в сети «Интернет» активно появляются и сайты фейковых банковских учреждений, например: «Банк социальной поддержки населения» (РФ) (http://soc-bank.ru) (рис. 8). В связи с очередным всплеском заболеваемости COVID-19 фиксируются также многочисленные случаи появления в сети ложных сайтов медицинского характера (например, по адресу: https://docs-docs.net), требующих при регистрации указать не только стандартные персональные данные (ФИО, дата рождения, адрес проживания и др.), но и сведения о банковской карте (номер, срок действия, CVV-код). Подобные сайты зачастую создаются на едином шаблоне, меняется лишь название и логотип.

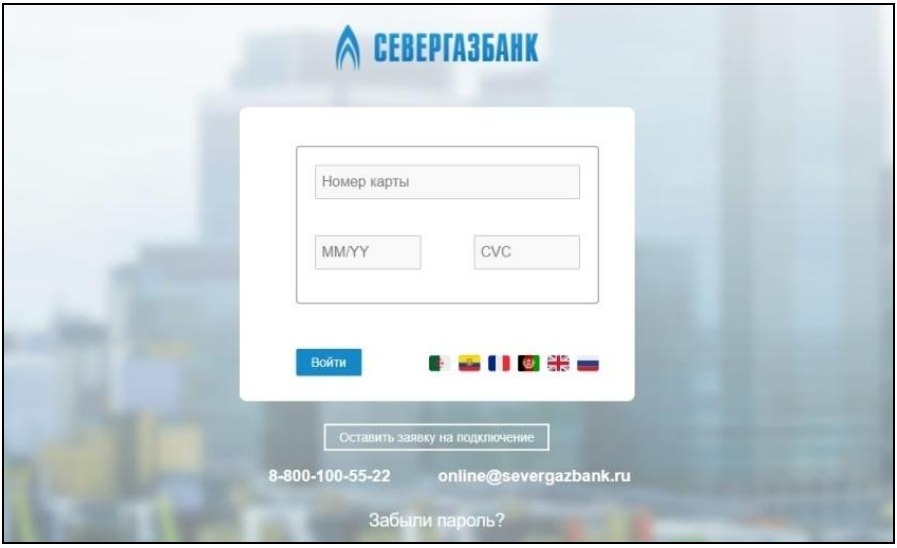

Рис.7. Фишинговый сайт «Севергазбанка» (РФ) (https://severogazbank.com)

Одним из способов совершения мошенничества с использованием ЭСП является *фарминг* (от англ. pharming – скрытное перенаправления на ложный IP-адрес). Его особенностью является подмена оригинального сетевого ресурса на мошеннический и скрытое перенаправление пользователя на поддельный сайт с целью завладения личными данными пользователя. Осуществляется посредством использования вредоносного программного обеспечения класса XSS (от англ. Cross-SiteScripting – «межсайтовый скриптинг»), осуществляющих внедрение в выдаваемую веб-системой страницу вредоносного кода, либо использования кэша DNS на конечном устройстве пользователя или на сетевом оборудовании провайдера услуг связи.

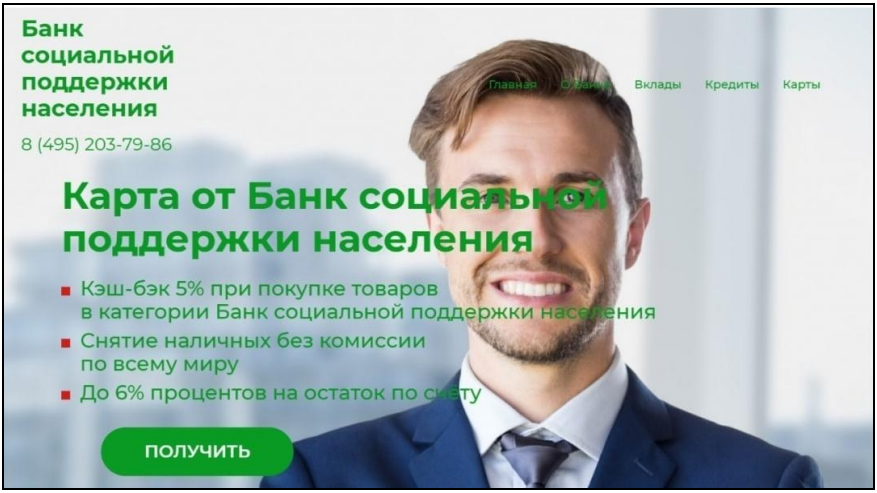

Рис. 8. Фишинговый сайт фейкового банка (http://soc-bank.ru)

Возможна также модификация системных настроек (например, перенастройка браузера на работу через троянский прокси-сервер или подмена DNS-сервера провайдера в настройках TCP/IP на мошеннический DNS-сервер).

Еще одним современным видом мошенничества, направленного на несанкционированное получение доступа к ЭСП является *взлом сети, составляющей «интернет вещей»* пользователя. Используя специальное программное обеспечение (например, поисковые системы Shodan и Censys), злоумышленники осуществляют поиск незащищенных ро-

утеров, IP-камер, элементов системы «умный дом», носимых смарт-гаджетов и других устройств, использующих установленные по умолчанию логины и пароли либо имеющих иные уязвимости. Затем, подключаясь к этим устройствам, они приобретают доступ к персональной информации владельца (сведения об аккаунте, цифровом окружении, домашней Wi-Fi-сети и т. п.), позволяющей выполнить скрытое перенаправление пользователя на мошеннический сайт.

Принимая сообщения от доверенных устройств в своей домашней сети, пользователь обычно не сомневается в их достоверности и переходит по вредоносным ссылкам либо выполняет иные действия, посредством которых мошенники получают неправомерный доступ к ЭСП потерпевшего.

При этом очевидно, что если бытовое уязвимое устройство (например, IP-камера либо «умный» холодильник) чаще всего ставит под угрозу сохранность частной жизни небольшой группы людей либо их денежных средств, то незащищенная в должной мере критически важная инфраструктура (например, медицинское оборудование в больницах, автоматизированная система управления промышленными объектами, бортовая система управления транспортом и т. д.) способны навредить значительно большему числу людей. В этой связи системные администраторы подобных систем особое внимание должны уделять вопросам технической защиты и обеспечения их безопасности.

Практическая реализация технических мер противодействия фишингу и фармингу носит преимущественно комплексный характер и базируется на ряде правил:

1. Антивирусная проверка подозрительных ссылок (URL) на предмет выявления ВПО. Для этого следует воспользоваться одним из онлайн-сервисов, например: VirusTotal (https://www.virustotal.com) (рис. 10). Отличительной особенностью указанного сетевого ресурса является то, что он использует данные 57 различных антивирусных баз (Avira, ComodoSiteInspector, Dr.Web, GoogleSafebrowsing, Kaspersky, ESET, Netcraft и др.) (рис. 9).

Рис. 9. Онлайн-сервис Virustotal.com для анализа подозрительных файлов и ссылок (URL)

Также возможна установка десктопного приложения VirusTotalUploader (https://www.virustotal.com/static/bin/vtuploader2.2.exe). С его помощью пользователь имеет возможность проверить не только подозрительные файл или ссылку, но и уже запущенные системные процессы (рис. 11).

Существуют также альтернативные онлайн-сервисы анализа подозрительных ссылок (URL) на предмет выявления ВПО. Так, онлайн-ресурс CheckShortURL (http://checkshorturl.com) предназначен для проверки коротких (сокращенных) ссылок, создаваемых большинством сервисов сокращения URL (рис. 12). Сервис позволяет выполнить предварительный просмотр сайта, чтобы убедиться в его благонадежности. Если у пользователя возникнут сомнения по поводу безопасности сайта, то с помощью CheckShortURL можно автоматически осуществить поиск сайта в различных сервисах по оценке безопасности, например таких, как WebofTrust.

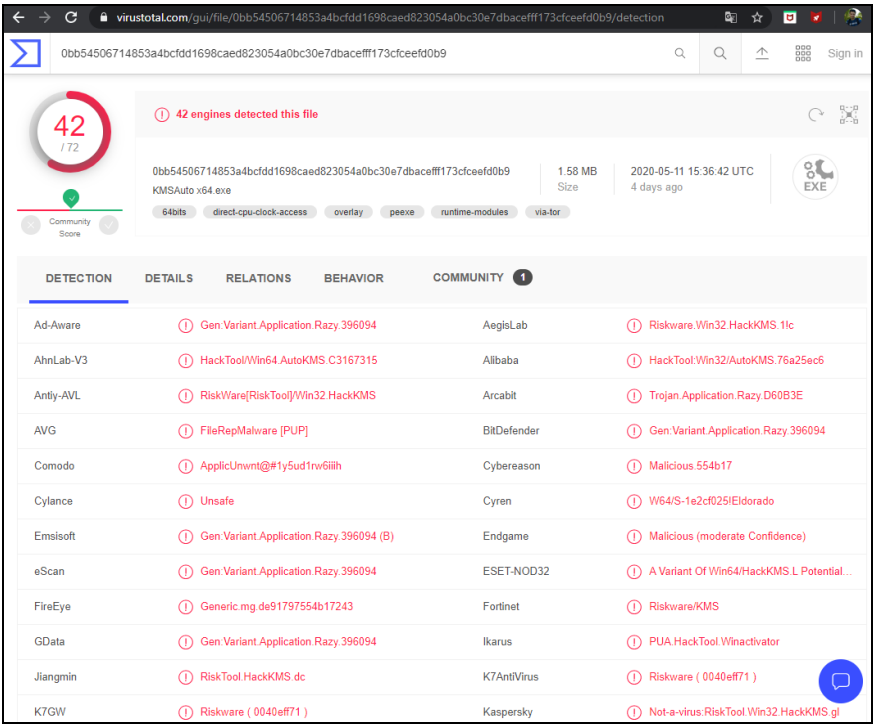

Рис. 10. Результаты проверки подозрительного файла с помощью онлайн-сервиса VirusTotal.

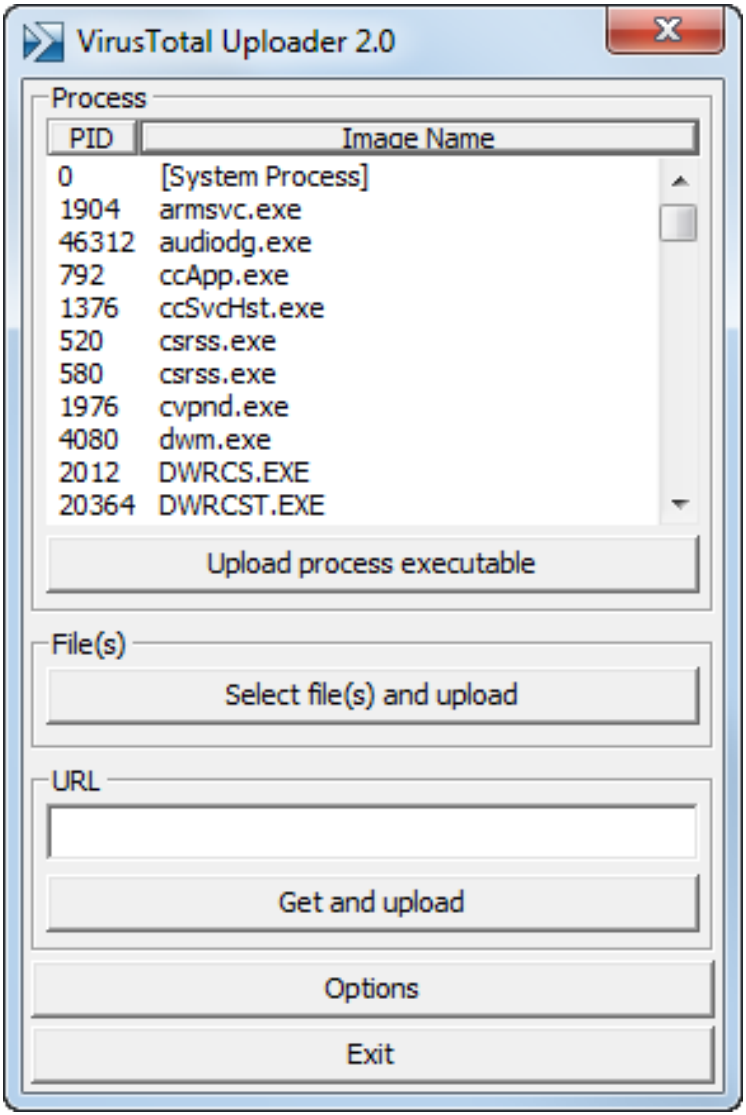

Рис. 11. Десктопное приложение VirusTotalUploader для анализа подозрительных файлов и ссылок (URL)

Рис. 12. Онлайн-сервис CheckShortURL для проверки ссылок (URL)(http://checkshorturl.com)

В случае, если необходимо узнать, что именно происходит в процессе переадресации и через какие этапы проходит переадресация при нажатии на короткую ссылку, целесообразно воспользоваться сетевым сервисом GetLinkInfo (http://getlinkinfo.com). Функциональные возможности этого ресурса основываются на технологиях безопасного просмотра, принадлежащих корпорации Google.

Рис. 13. Онлайн-сервис GetLinkInfo (http://getlinkinfo.com) для проверки ссылок URL

Кроме того, некоторые сервисы сокращения URL предоставляют возможность проверки сгенерированных на их сайте ссылок, чтобы пользователям не приходилось идти на риск. Например, если добавить «+» к концу ссылки Bit.ly, то пользователь перейдет на страницу предварительного просмотра перед тем, как перейдет к самому файлу или сайту. Например: *http://bit.ly/1dNVPAW*+.

В целях проведения оперативного онлайн-анализа файлов и ссылок на мобильных устройствах рекомендуется использовать специальные боты[1] в интернет-мессенджерах (например, для Telegram: @drwebbot (https://telegram.me/drwebbot) (рис. 14).

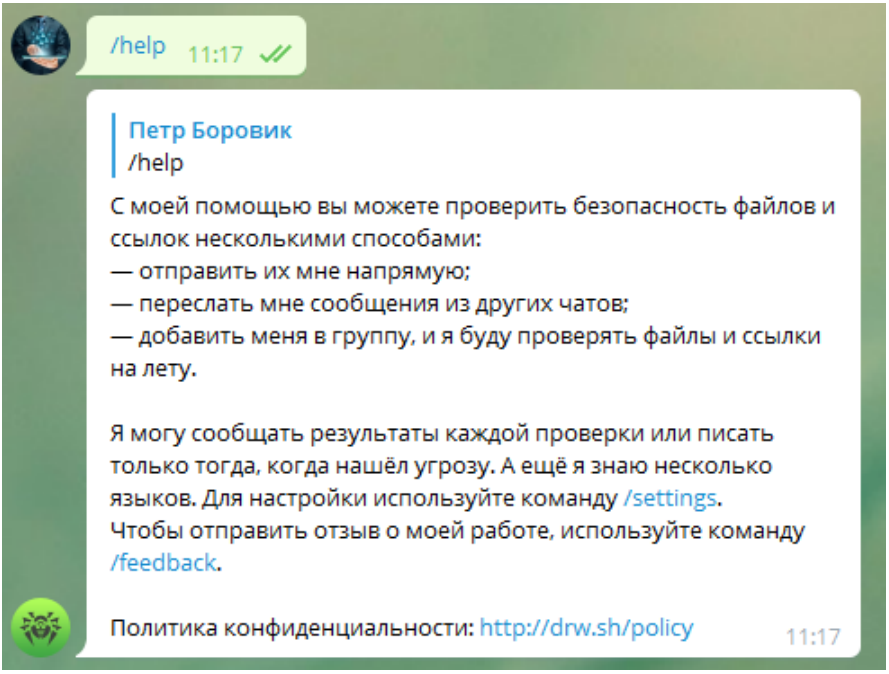

Рис. 14. Онлайн-сервис (бот) @drwebbot (https://telegram.me/drwebbot) для проверки ссылок URL на мобильном устройстве

[1] Бот – специальный аккаунт в Telegram, созданный для того, чтобы автоматически обрабатывать и отправлять сообщения. Пользователи могут взаимодействовать с ботами при помощи сообщений, отправляемых через обычные или групповые чаты.

Для предотвращения вредоносных атак с использованием эксплойтов (уязвимостей) уровня ядра, запускающих вредоносное программное обеспечение с наивысшими привилегиями (например, *WannaCry* и *Petyaransomware*), пользователю операционной системы Windows 10 рекомендуется активизировать функции «Изоляция Ядра» и «Целостность памяти» центра защиты WindowsDefender.

Функция «Изоляция ядра» обеспечивает дополнительную защиту от ВПО, изолируя процессы компьютера от операционной системы и устройства. Функция «Целостность памяти» запрещает вредоносному коду доступ к процессам с высоким уровнем безопасности в случае атаки. Однако для включения данных функций аппаратное обеспечение компьютера должно поддерживать технологию виртуализации, позволяющую компьютеру с Windows 10 запускать приложения в контейнере, изолированном от критически важных частей системы.

2. *Проверка whois-данных* исследуемого сайта (домена), позволяющая произвести простейший контроль: как давно зарегистрирован сайт магазина, есть ли у него юридический адрес, телефоны, e-mail и т. п.

Для предоставления указанных сведений существует ряд сетевых whois-ресурсов (от англ. «whois» – «кто такой»). Популярным среди них является CentralOps.net (http://centralops.net). Среди русскоязычных сервисов наиболее удобными являются http://2ip.ru/, https://whois.ru и др. (рис. 15).

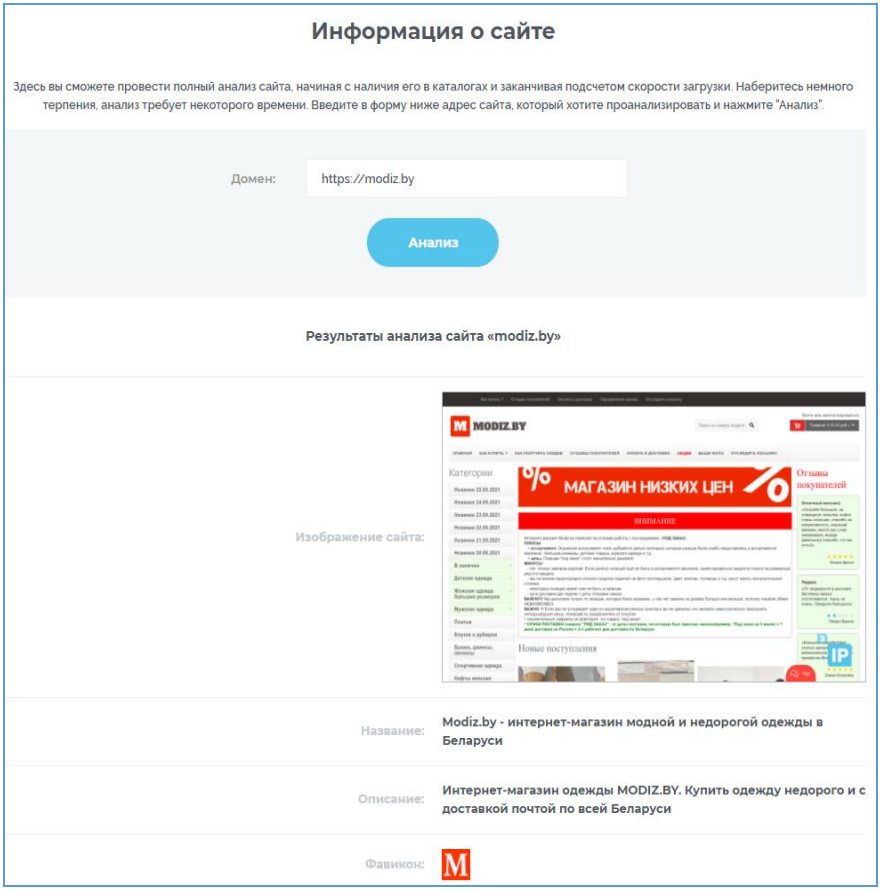

Рис. 15. Сетевой whois-ресурс (http://2ip.ru). Часть 1

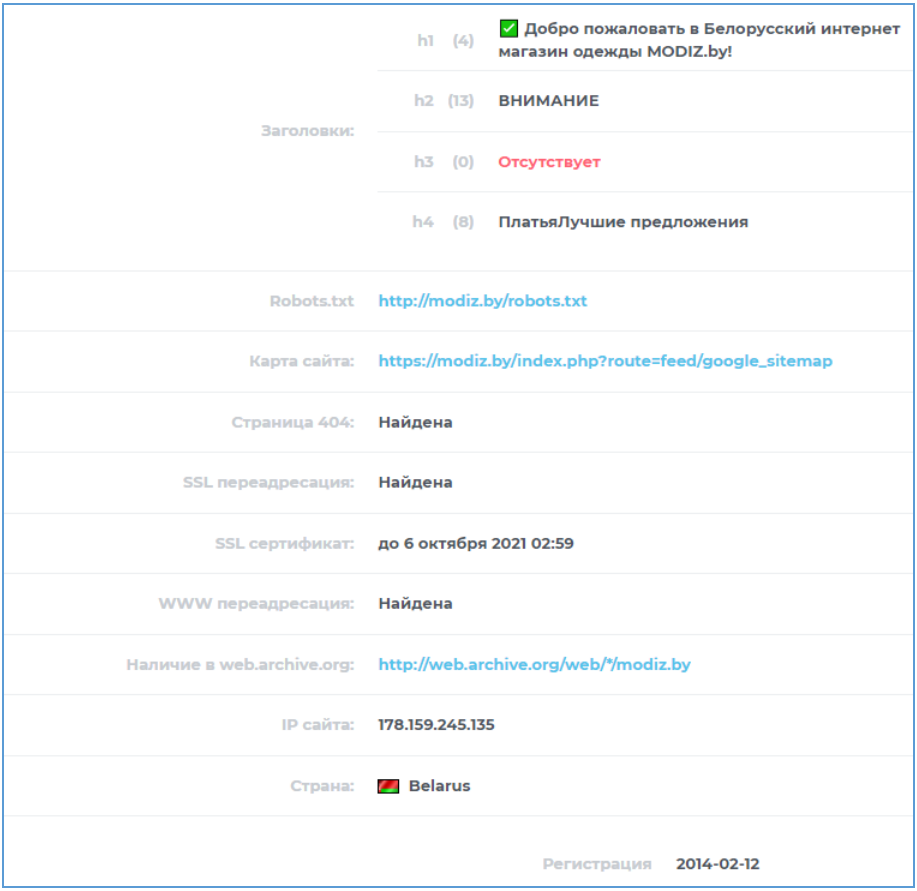

Рис. 16. Сетевой whois-ресурс (http://2ip.ru). Часть 2

Технические меры противодействия *взлому сети, образующей «интернет вещей»* пользователя, также носят комплексный характер и должны быть направлены в первую очередь на обеспечение защиты центрального компонента такой сети – Wi-Fi-роутера. Для реализации такой защиты рекомендуется:

1) установить надежный пароль для доступа к роутеру (длинный нестандартный ключ от 15–20 символов и выше, в котором будут заглавные буквы, цифры и специальные знаки: ~ ! @ # $ % & *);

2) задать уникальное нераспространенное имя (SSID) для сети Wi-Fi. Для взлома беспроводной сети злоумышленники часто используют

метод полного перебора предполагаемых паролей, осуществляемого путем последовательного пересмотра всех слов (паролей в чистом виде или их зашифрованных образов) определенного вида и длины из словаря – так называемой «радужной» таблицы *(rainbowtable)*, в которой хранятся миллионы возможных паролей и их комбинаций. Если имя SSID и пароль находятся в такой таблице, злоумышленник с помощью специальных программ сможет мгновенно получить доступ к сети;

3) сделать Wi-Fi-сеть «невидимой», исключив ее из списка доступных беспроводных сетей. Для этого необходимо в настройках роутера включить опцию «Скрыть SSID» либо «Отключить широковещание SSID». Это позволит обеспечить дополнительный уровень защиты: при подключении к такой сети нужно будет указать не только пароль, но и имя самой сети (SSID);

4) включить шифрование WPA2 (AES). При работе в беспроводной сети со слабым шифрованием передаваемые критически важные данные могут быть перехвачены злоумышленниками. К распространенным типам шифрования относятся WEP, TKIP, WPA, WPA2 (AES). Последний из них является наиболее надежным;

5) отключить технологию WPS, позволяющую подключать сетевые устройства к роутеру без пароля;

6) включить фильтрацию по MAC-адресам для доверенных устройств, т. е. составить белый список уникальных адресов Wi-Fi адаптеров (сетевых карт) устройств, которым разрешено подключаться к сети. Один из самых эффективных способов защиты маршрутизатора;

7) в параметрах локальной сети LAN-роутера отключить DHCP-сервер, а затем изменить используемую подсеть (для этого необходимо поменять его IP-адрес, т. е. вместо стандартного 192.168.1.1 или 192.168.0.1 следует ввести другой, уникальный). Благодаря этому действию пользователи сети не будут автоматически получать адреса, а вынуждены будут указывать их вручную. Не зная IP-адреса, маску подсети и шлюза, злоумышленник, даже подключившись к сети через сетевой кабель, не сможет получить к ней доступ;

8) отключить ответы на команды *Ping* (удаленная проверка целостности и качества соединений в сетях на основе TCP/IP);

9) уменьшить мощность (радиус распространения) сигнала Wi-Fi до значения, когда сигнал сети будет приниматься только в пределах вашего помещения. Уменьшенный радиус сигнала беспроводной сети

существенно снизит вероятность подключения к ней посторонних лиц;

10) активизировать межсетевой экран на маршрутизаторе (при его наличии). С его помощью закрыть все порты, за исключением необходимого минимума;

11) использовать технологию VPN[1] на маршрутизаторе (при ее наличии);

12) заблокировать удаленный (через Интернет) доступ к роутеру;

13) регулярно обновлять прошивку роутера. Это позволит минимизировать ошибки и уязвимости типа *backdoor,* повысить надежность и стабильность устройства;

14) осуществлять проверку на наличие чужих (не доверенных) устройств в списке подключенных клиентов на вашем роутере;

15) при работе в беспроводной сети использовать только защищенное соединение HTTPS (проверять, чтобы в адресной строке браузера была зеленая или серая иконка замка);

16) при работе с операционной системой Windows рекомендуется выключить службу общего доступа к файлам и принтерам для всех публичных сетей.

В контексте растущей общественной опасности преступлений рассматриваемой категории особое значение приобретает *мошенничество в системах ДБО*. Если еще несколько лет назад основные угрозы для банков и платежных систем были преимущественно связаны со скиммингом[2] и кардингом[3], то сегодня фокус внимания злоумышленников все чаще направлен в сторону высокотехнологичных банковских систем. Это связано не только с резким возрастанием уровня профессиональных умений и навыков у лиц, занимающихся хищением денежных средств с электронных счетов граждан, но и появлением более широкого спектра возможностей по «заметанию» следов совер-

[1] VPN (Virtual Private Network) – виртуальная частная сеть, которая позволяет объединять компьютерные устройства в защищенные сети, чтобы обеспечивать их пользователям зашифрованный канал для безопасной передачи данных между устройством и сервером.

[2] Скимминг (от англ. skimming) – кража данных карты при помощи специального считывающего устройства (скиммера).

[3] Кардинг (от англ. carding) – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны»).

шенного криминального деяния, маскировке способов его подготовки и совершения.

Различные методы мошенничества указанного вида нередко могут быть классифицированы как одна из форм фишинга. Вместе с тем с точки зрения практической реализации мошенничество в системах ДБО основано на получении несанкционированного доступа к пользовательской информации, необходимой для авторизации и последующего хищения денежных средств со счетов пользователей. Злонамеренные действия злоумышленников обычно основываются на различных способах использования ВПО. К наиболее распространенным из них относятся:

1. «Заражение» ВПО компьютера с системой ДБО пользователя посредством целевой рассылки электронных писем. В их тексте обычно приводятся и обосновываются причины для открытия файла с вирусом, прилагаемого к письму (например, с просьбой проверки документов финансового характера, статистической отчетности и пр.).

После открытия вложенного файла ВПО внедряется в систему пользователя и сообщает на удаленный сервер злоумышленника свой статус об успешной установке. Этот метод актуален для проведения целевых атак, когда у мошенника имеются адреса электронной почты лиц, работающих с системой ДБО.

2. Эксплуатация уязвимостей на тематических сайтах (например, «Клерк.ру», «Audit – it.ru», «Бухгалтерия онлайн», «Бух. 1С», «В помощь бухгалтеру» и др.).

Данный метод является одним из наиболее эффективных, поскольку дает возможность выполнять массовое распространение ВПО с учетом конкретной целевой аудитории.

Схема атаки обычно состоит из следующих действий:

– осуществляется компрометация соответствующего тематического сайта;

– в сайт встраивается вредоносный программный код, который вместе с содержимым сайта загружает вредоносные компоненты;

– при посещении пользователями такого сайта злоумышленником осуществляется анализ их программно-аппаратного окружения (операционная система, установленные компоненты, браузер и его плагины и др.). В случае обнаружения осуществляется загрузка и запуск заданной вредоносной программы;

– после запуска вредоносной программы на удаленный сервер злоумышленника сообщается статус об успешной установке;

– злоумышленник проверяет на сервере появление новых событий от распространяемых им программ.

Последующие действия мошенников обычно направлены на закрепление в системе, дальнейшее хищение ключевой информации, а также получение удаленного управления компьютером[1].

По мнению специалистов, одними из наиболее распространенных уязвимостей тематических сайтов, находящихся в фокусе мошеннических действий, являются следующие недостатки:

– недостаточная проверка входных данных;

– раскрытие чувствительной информации;

– использование паролей недостаточной сложности[2].

С развитием информационно-коммуникационных технологий одной из распространенных разновидностей рассмотренного способа мошенничества стало *создание поддельных платежных систем и форм экспресс-оплаты*. Осуществляя взлом систем защиты популярных онлайн-сервисов (интернет-магазины, электронные сервисы объявлений, торговые площадки и пр.), мошенники создают ложные формы оплаты, через которые получают денежные средства пользователей, оплачивающих различные услуги.

Для маскировки вышеприведенных мошеннических действий злоумышленники используют различные приемы и методы, основанные на применении анонимных прокси-серверов, позволяющих скрывать реальный IP-адрес, а также сетевых атаках класса *DoS* (от англ. DenialofService – отказ в обслуживании), с помощью которых блокируется легитимный доступ пользователей к системным ресурсам.

Дополнительным стимулом, способствующим росту представленных способов мошенничества, является стремительное и повсеместное распространение мобильных устройств, оснащенных клиентскими приложениями ДБО. При этом открытость и уязвимость встроенных операционных систем (например, Android), наряду с интегрированными возможностями управления информационной безопасностью непосредственно клиентами системы ДБО, формируют благоприятные условия для совершения преступлений рассматриваемого вида.

---

[1] См.: *Лямин Л., Пятиизбянцев Н., Пухов А.* Указ. соч. С. 56.

[2] Анализ защищенности web-приложений. URL: https://www.group-ib.ru/audit/web-apps.html.

Логично предположить, что наблюдаемый в настоящее время массовый характер мошенничеств в обозначенной сфере должен был бы мотивирость руководство финансовых и банковских организаций к наращиванию потенциала программно-технической защиты в данном направлении. Тем не менее, несмотря на растущие финансовые потери, отдельные аспекты этой деятельности (их рассмотрение не является предметом нашего исследования) требуют совершенствования.

Очевидно, что для противодействия мошенничеству в системах ДБО недостаточно применять только лишь средства антивирусной защиты, межсетевые экраны или шифрование. Исследование показало, что меры противодействия указанным уголовно-наказуемым деяниям должны не только учитывать самые современные подходы к общепринятому программно-техническому обеспечению информационной безопасности, но представлять собой взаимосвязанную систему мероприятий, направленных на *обнаружение*, *предотвращение* и *пресечение* действий злоумышленника.

Учитывая вышеизложенное, а также руководствуясь результатами анализа публикаций по рассматриваемой тематике и соответствующей правоприменительной практики, система технических мер противодействия мошенничеству в системах ДБО должна включать в себя следующие подсистемы реагирования и защиты:

1. Средства обнаружения сетевых атак – современные программно-технические решения, имеющие комплексный характер и сочетающие в себе различные инструменты, позволяющие осуществлять мониторинг, обнаружение и анализ происходящих в информационных системах изменений в целях своевременного выявления сложных целенаправленных атак и полноценного анализа произошедших событий.

Рассмотрим основные виды средств обнаружения, которые являются актуальными и востребованными в настоящее время.

1.1. *Межсетевые экраны*[1] – средства межсетевой защиты, способные разделить компьютерную сеть на две части (внутреннюю и внешнюю) и реализовать набор правил прохождения сетевых пакетов с данными через границу одной части сети в другую.

[1] Другие названия: Брандмауэр (*нем.* Brandmauer – противопожарная стена) – заимствованный из немецкого языка термин; Файрволл (*англ.* Firewall – противопожарная стена) – заимствованный из английского языка термин.

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Наиболее распространенное место для установки межсетевых экранов – граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов – в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечет границу сетевого периметра и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности[1].

Фильтрация трафика осуществляется на основе набора предварительно сконфигурированных правил, которые называются *ruleset*. Удобно представлять межсетевой экран как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельного правила. Последовательность правил в наборе существенно влияет на производительность межсетевого экрана. Например, многие межсетевые экраны последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие. Для таких межсетевых экранов правила, которые соответствуют наибольшему количеству трафика, следует располагать как можно выше в списке, увеличивая тем самым производительность.

Межсетевые экраны нового поколения сочетают в себе функции как классического межсетевого экрана, так и более продвинутые технологии, применяемые в различных сочетаниях:

– межсетевое экранирование прикладного уровня;

– сигнатурный анализ трафика для обнаружения угроз и их блокирования;

– полнотекстовый анализ (инспекция) трафика, зашифрованного протоколами различного уровня;

– возможности по ограничению и приоритезации трафика;

[1] См.: *Лебедь С. В.* Межсетевое экранирование. Теория и практика защиты внешнего периметра. М., 2002. С. 127.

– поведенческий анализ файлов в изолированной среде («песочницы»);

– регулярные обогащения данными об актуальных угрозах (репутационные списки, индикаторы компрометации и т.п.).

Существует два варианта исполнения межсетевых экранов – программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант имеет две разновидности – в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

1.2. *Системы мониторинга событий безопасности (Security Informationand Event Management, SIEM-системы)*. Программные решения данного вида отслеживают и анализируют в режиме реального времени события, поступающие от информационных систем, сетевых устройств и приложений (в том числе и территориально удаленных), входящих в инфраструктуру ДБО. Выступают в качестве управляющего и интегрирующего звена, находящегося поверх существующей системной инфраструктуры и программных средств безопасности.

Средства SIEM позволяют выполнять следующие задачи:

–сбор и анализ больших объемов событий информационной безопасности (инструменты SIEM объединяют журналы событий и системы, а также данные о безопасности из различных источников и приложений в одном месте);

– мониторинг текущего состояния средств защиты программно-технической инфраструктуры ДБО, обнаружение компьютерных инцидентов в режиме реального времени;

– реагирование на сбои в работе средств обеспечения информационной безопасности в системе ДБО;

– построение топологической карты сетевой инфраструктуры сети ДБО для прогнозирования вредоносных атак, а также анализа и оценки рисков в режиме реального времени;

– управление идентификацией и доступом.

Программные инструменты SIEM играют важную роль в повышении эффективности и своевременности действий по реагированию на инциденты безопасности. При обнаружении нарушения служба безопасности может использовать программное обеспечение SIEM, чтобы быстро определить, как произошла атака и какие хосты или приложения были затронуты нарушением.

1.3. *Системы анализа сетевого трафика*. Предназначены для выявления вредоносных атак в компьютерной сети путем перехвата и анализа сетевого трафика в режиме реального времени. Помогают раскрыть присутствие злоумышленников на ранней стадии мошеннической атаки на сервер с системой ДБО и оперативно нейтрализовать выявленные угрозы. При выявлении подозрительных попыток подключения с неавторизованного узла на контроллер домена указанные системы позволяют выполнить анализ исторических данных сетевой активности узла и установить дополнительные сведения об инциденте.

Решение задачи анализа сетевого трафика основывается на комплексном подходе и состоит из ряда относительно независимых подзадач (рис. 17): перехват трафика, его хранение и анализ.

Перехват трафика осуществляется с помощью снифферов – программных (программно-аппаратных) средств, устанавливаемых как на маршрутизаторе, так и на оконечном узле сети. Данная задача может осуществляться:

– с помощью «прослушивания» сетевого интерфейса;

– подключением сниффера в разрыв канала;

– посредством анализа побочных электромагнитных излучений;

– через атаку на канальном или сетевом уровне, приводящую к перенаправлению трафика исследуемого хоста на сниффер.

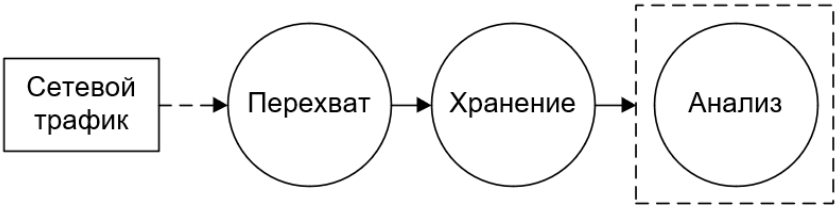

Рис. 17. Подзадачи системы анализа сетевого трафика

Исходя из специфики подзадач, которые необходимо решить, анализ сетевого трафика обычно реализуется в двух направлениях. Первое из них основывается на восстановлении сессии и разборе заголовков сетевых протоколов (базовый анализ). Второе – направлено на решение достаточно специфических задач, требующих индивидуаль-

ного подхода к выбору программно-технического инструментария, например:

– анализ туннелированных протоколов произвольной глубины;

– анализ сессий на уровне приложений (выделение связей между потоками данных, передаваемых по сети);

– выполнение определенных сценариев (скриптов) в случае обнаружения в трафике предварительно заданных сигнатур[1].

1.4. *Системы выявления и учета компьютерных угроз (ThreatIntelligencePlatform, TIP-системы)*. Класс решений этого вида представляет собой специализированную платформу, предназначенную для обогащения, обнаружения, распространения и корреляции данных об угрозах. Позволяет проводить развернутую аналитику по уязвимостям и угрозам в защищаемой информационной системе. Имеется возможность централизованной обработки любых доступных источников информации об угрозах, а также интеграции с другими инструментами в области информационной безопасности (SIEM-системы, системы анализа сетевого трафика, средства поведенческого анализа, реагирования на инциденты и т д.).

Технология TIP основывается на проактивном поиске следов компрометации или признаков вредоносной атаки с целью обнаружения и пресечения угрозы. При этом данный процесс выполняется не после факта обнаружения либо срабатывания системы защиты, а в режиме реального времени в ходе работы аналитика.

Важным элементом TIP-систем является собственная база знаний центра реагирования, призванная накапливать данные по результатам расследований.

1.5. *Средства обнаружения компьютерных атак на конечных устройствах (Endpoint Detection & Response, EDR)*. Программные решения этого вида направлены на выявление и обнаружение вредоносных атак на конечные устройства пользователей (компьютеры, смартфоны, планшеты и т п.), подключенных к системе ДБО. В отличие от антивирусов, задача которых бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз, которые нацелены на обход традиционных средств защиты.

[1] См.: Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика. URL: https://www.ispras.ru/preprints/docs/prep_27_2014.pdf.

В общем случае системы класса EDR состоят из программ-агентов, устанавливаемых на конечные точки, и серверной части. Программа-агент осуществляет мониторинг запущенных процессов, действий пользователя и сетевых коммуникаций, после чего передает информацию на локальный либо облачный сервер. Серверный компонент анализирует полученные данные при помощи технологий машинного обучения, сопоставляет их с базами индикаторов компрометации и другой доступной информацией о сложных угрозах. Если EDR-система обнаруживает событие с признаками преступления, она оповещает об этом сотрудников службы безопасности. Это способствует своевременному принятию необходимых мер по блокировке вредоносной атаки (например, закрытию скомпрометированных портов, изоляции атакованного сетевого сегмента, прерывания доступа к веб-сервису и т. п.).

Большинство современных EDR-решений позволяют:

– осуществлять сбор данных с конечных устройств в режиме реального времени;

– записывать и хранить информацию о действиях пользователей, сетевой активности и запущенных программах для последующего изучения и исследования;

– выявлять и классифицировать подозрительную активность, а также уведомлять службы безопасности о ней;

– предпринимать шаги по блокировке атаки – изолировать подозрительные файлы, останавливать вредоносные процессы, разрывать сетевые соединения;

– интегрироваться с защитными решениями для конечных точек, SIEM-системами и другими средствами защиты;

– выполнять проактивный поиск угроз, анализируя нетипичное поведение и подозрительную активность[1].

1.6. *Система анализа сетевого трафика нового поколения*. Данные программные инструменты предназначены как для анализа сетевого трафика, так и поведенческой аналитики. Это дает возможность в автоматическом режиме реагировать на угрозы посредством интеграции с различными средствами управления информационной безопасностью (межсетевые экраны, средства управления доступом к сети,

[1] Endpoint Detection & Response (EDR). URL: https://encyclopedia.kaspersky.ru/glossary/edr-endpoint-detection-response.

SIEM-системы и т. п.), а также проводить расследование инцидентов и поиск угроз в собираемых исторических метаданных.

1.7. *Средства поведенческого анализа («песочницы»)*. Представляют собой программные инструменты создания изолированных сред для безопасного запуска исполняемых файлов. Обычно частично эмулируют либо ограничивают доступ к сети, а также считывание информации с устройств ввода. Используются для анализа файлов на предмет наличия ВПО либо запуска подозрительного кода. Помогают аналитикам оперативно проводить эвристический, а также поведенческий анализ выполняемых проверяемым объектом операций с целью своевременного выявления потенциальных угроз. С целью совершенствования применяемых методов рекомендуется интеграция с другими классами решений по обнаружению угроз и защите информационного контура.

К основным функциям средств поведенческого анализа относятся:

а) обнаружение и предотвращение целевых атак и неизвестных ранее вредоносных программ. На основе результатов эмуляции в виртуальной среде осуществляется блокирование файлов и электронных сообщений.

б) облачная проверка электронных сообщений и вложений на наличие угроз;

в) постоянное обновление сигнатур (сведений о потенциально опасных объектах). Как только в одной из песочниц будет выполнена эмуляция неизвестного ранее вредоносного кода, его сигнатуры попадут в общую базу;

г) мониторинг безопасности (анализ уровня защищенности и подготовка отчета по выявленным угрозам).

Принцип функционирования программных средств поведенческого анализа можно описать следующим образом (рис. 18). Анализируемые файлы попадают в очередь на предварительную проверку средствами защиты первого рубежа (резидентные антивирусные программы на межсетевых экранах, на рабочих станциях). Если в ходе предварительной проверки вредоносные программы не обнаружены, объект помещается в виртуальную машину и исполняется там. В виртуальной машине нет специализированного инструментария для анализа – имеются только стандартный набор программ обычного офисного автоматизированного рабочего места и доступ в сеть «Интернет» для детектирования сетевой активности. Все действия исследуемой про-

граммы внутри виртуальной машины через гипервизор попадают в анализатор, который должен понять, происходит ли что-то вредоносное, опираясь на имеющиеся у него шаблоны поведения. Контекст и результаты анализа заносятся в базу данных для хранения, дальнейшего использования и обучения анализатора[1].

Средства поведенческого анализа могут быть встроены в другие сетевые устройства безопасности – межсетевые экраны, системы предотвращения вторжений, прокси-серверы с интегрированным потоковым антивирусным модулем, почтовые и веб-шлюзы. Наиболее предпочтительным вариантом внедрения средства поведенческого анализа является использование отдельных устройств и их тесная интеграция с элементами сетевой инфраструктуры.

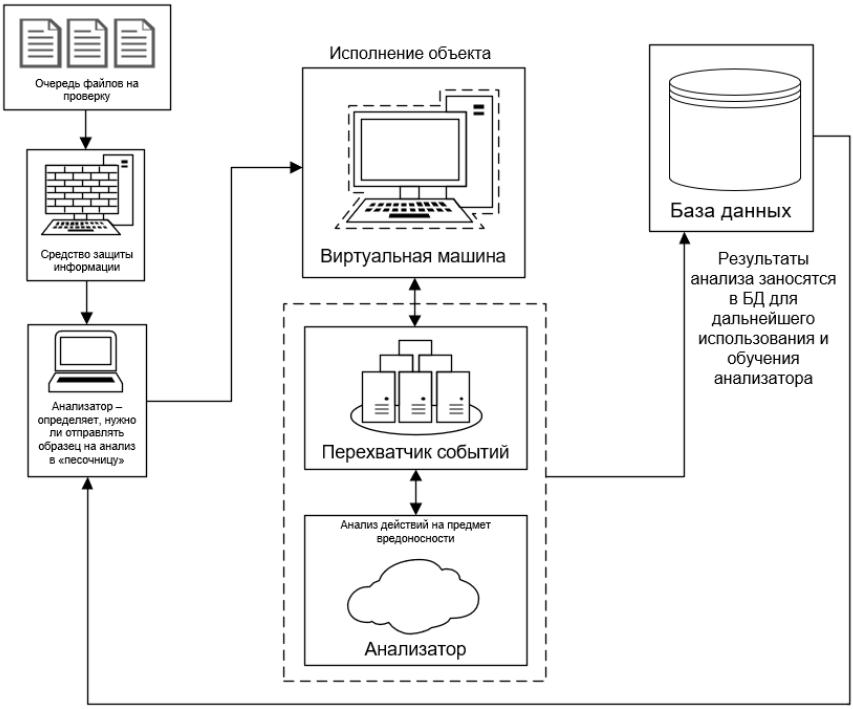

Рис. 18. Принцип действия средства поведенческого анализа («песочницы»)

[1] См.: *Олиндер Н. В.* Указ. соч.

1.8. *Приманки для хакеров («Honeypot»)*. Решения этого класса позволяют выявлять попытки вредоносных атак с целью взлома, осуществлять их прогнозирование, принимать меры оперативного реагирования. В качестве «приманки» обычно используют изолированные от критически важных информационных систем веб-сервера, виртуальные машины либо иные сетевые устройства со специально открытыми портами и уязвимостями. Внутри защищаемого пространства, предназначенного для раскрытия атакующих, размещают различные ресурсы, замаскированные под важные файлы, почтовые сообщения, данные учетных записей, ссылки, призванные вызвать интерес у злоумышленников.

Для противодействия фишинговым атакам и деанонимизации злоумышленников активно применяют так называемые IP-ловушки – специальные honeypot-ссылки, встраиваемые в код веб-сайта и позволяющие оперативно раскрывать исчерпывающую информацию о попытке взлома (дата/время, IP-адрес, UserAgent[1] и т. д.).

2. Подсистема мониторинга и оценки транзакций в платежной системе «Антифрод» (от англ. anti-fraud «борьба с мошенничеством»). Является современным технологическим решением в области минимизации рисков, связанных с проведением мошеннических операций по банковским картам, позволяющим фильтровать подозрительные и мошеннические операции, по минимуму влияя на конверсию успешных платежей. Обычно представляет собой платформу управления более чем двумястами различными правилами и параметрами, позволяющими гибко подстраиваться под специфику конкретной бизнес-модели. Встроенные фильтры помогают распознать необычное поведение и оценить риски транзакции, после чего применить меры для разрешения или запрета ее осуществления.

Антифрод-система – это система мониторинга и предотвращения мошеннических операций, которая в режиме реального времени проверяет каждый платеж, применяя множество фильтров.

Практически все платежные системы и платежные агрегаторы обладают своими антифрод решениями. Цель антифрод-системы заключается в том, чтобы убедиться, что, например, пользователь является

[1] User Agent – в общем виде сведения о браузере, его версии, используемом устройстве, операционной системе и механизме веб-рендеринга.

реальным владельцем платежной карты, совершающим покупку в интернет-магазине. В случае выявления подозрительной активности, то есть превышения какого-либо значения параметра, система автоматически блокирует возможность совершения платежа либо отправляет покупателя на дополнительную проверку.

Преступники стараются, чтобы их цифровой след максимально совпадал с цифровым следом владельца аккаунта (платежной карты) и ставят цель быть максимально похожими на реального покупателя со всеми возможными данными с учетом чего и совершают хищение.

Общий механизм работы антифрод-системы можно свести к следующему:

– сервер банка переадресовывает сведения о транзакции в антифрод-систему и ожидает разрешения на проведение платежа;

– антифрод-система анализирует сведения, чтобы принять решение о легитимности этой транзакции;

– обрабатывается платеж, оценивается его риск, при необходимости инициируется проверка другими сервисами, например, дополнительная аутентификация клиента, и передается обратно решение. В результате чего финансовая транзакция оказывается подтвержденной или отклоненной.

Примером параметров, которые анализирует данная система, могут быть: страна платежной карты и IP-адрес плательщика; банк плательщика и получателя средств; количество платежей и их сумма за определенный отрезок времени; поддержка защищенного протокола авторизации «3-D Secure» или его отсутствие; телефон, E-mail, почтовый адрес, паспортные и иные персональные данные, статус идентификации клиента ДБО; история предыдущих транзакций; подозрительная активность. Также в момент совершения финансовой транзакции также анализируется User-Agent и сопоставляется с имеющимися в базе данных цифровыми отпечатками, куки-файлы на предмет подозрительной активности, а также собирается несколько показателей (у каждой антифрод-системы они различные) – начиная от IP-адреса компьютера, версии браузера и заканчивая статистикой платежей и др. Осуществляется проверка на использование виртуальной машины или VPN, анализируется поведение клиента, устанавливается наличие аккаунтов в социальных сетях на зарегистрированную электронную почту, проверяется информация о платежной системе, используется собственная база мошеннических действий. В особенных случаях сис-

тема может направлять платеж на дополнительную проверку или к антифрод-аналитику, который в ручном режиме контролирует подозрительность платежа и принимает окончательное решение по транзакции.

Система имеет набор правил, то есть фильтров безопасности. Фильтры антифрод-системы различные, например, географический (сверяет место положение по IP-адресу с местоположением владельца аккаунта (платежной карты), чем больше разница в расстоянии, тем выше подозрительность платежа); стоп-лист (некоторые аккаунты или платежные карты могу попадать в стоп-лист (например, когда владелец сообщил информацию о компрометации в банк); соответствие параметров (например, когда аккаунт (платежная карта), с которого происходит оплата, не походит под IP-адрес и настроенную операционную систему) и другие.

Другими словами, принцип работы антифрод-системы основывается на ряде следующих операций. Каждая транзакция сначала проходит через первую «линию обороны»: она проверяется на соответствие установленным ограничениям, таким как лимит на объем покупок по платежной карте, максимальную разовую сумму покупки, число пользователей одной карты, количество карт у одного клиента и др. Если все эти проверки прошли успешно, то запускаются следующие, более серьезные. По их результатам подсистема мониторинга и оценки транзакций присваивает транзакции одну из условных «меток»[1]:

Красная. Такая метка сигнализирует о реальной опасности мошенничества и выставляет обязательное требование аутентификации владельца платежной карты. Автоматически присваивается транзакциям с нестандартными характеристиками (например, пользователь из Испании оплачивает покупку в белорусском интернет-магазине картой, выпущенной в Великобритании).

Желтая. Сигнализирует о возможном факте мошенничества (например, если размер финансовой операции существенно выше среднего для конкретного интернет-магазина), рекомендует дополнительную проверку.

Зеленая. Отражает минимальную вероятность мошеннических действий (например, когда транзакция осуществляется в рамках одной

[1] Что такое антифрод: задачи и методы. URL: https://fisgroup.ru/blog/antifraud-zadachy-i-metody.

страны, а сумма денежного перевода является средней) и как следствие – одобрение транзакции.

Системой-антифрод к подозрительным относятся операции, когда с одного аккаунта совершается много неудачных покупок; один аккаунт – много IP-адресов и наоборот; платеж с одного аккаунта, но с разных устройств; различие в адресе клиента и доставки; оплата в ночное время по времени клиента, быстрые покупки, ввод текста путем копирования, смена пароля, адреса и других данных на аккаунте и т. д.

Если происходит отказ платежа, то причинами могут быть, например, определение транзакции как мошеннической, произошла ошибка заполнения платежных данных или нехватка средств.

В литературе предлагается ряд качественных и количественных критериев, которым должна соответствовать анифрод-система. При выборе системы фрод-анализа каждый субъект (например, банк) самостоятельно определяет, какие характеристики антифрод-системы для него наиболее важны. Тем не менее можно привести ряд критериев, на которые обращается внимание: срок существования анифрод-системы на банковском рынке, а также отзывы других банков; доступность внедрения и эффективность ее использования; возможности и готовность поставщика модифицировать систему под нужды конкретного банка; наличие интеграции с системой ДБО, внешними поставщиками информации; технологическая платформа и интеграционные возможности общесистемного программного обеспечения (операционная система, СУБД, сервера приложений), масштабируемость и т. д.; затраты на запуск и поддержание в процессе эксплуатации антифрод-системы (стоимость лицензии, поддержки); возможность оперативного произведения модификации антифрод-системы под специфичные запросы банка. Эффективная система фрод-анализа позволяет свести к минимуму риски хищений[1].

Для провайдера антифрода важна не только защита от мошенничества, но и минимизация ложных срабатываний. Исходя из сравнения существующих антифрод-систем, анализа положительных и отрицательных характеристик различных из подходов, целесообразна реализация системы, построенной на основе машинного обучения. Анти-

[1] См.: Варламова С. Б. Оптимизация расчета величины операционного риска // Финансовые рынки и банки. 2019. № 1. С. 36–44.

фрод-система должна быть максимально гибкой и настраеваемой, так как единого решения не существует.

В свою очередь необходимо отметить, что при оплате товаров или услуг в сети «Интернет» все чаще используется криптовалюта, а анализ практики противодействия киберпреступности свидетельствует о возможности активного использования криптовалют в преступной деятельности. Внедрение технологии блокчейн, цифровых знаков в определенной степени ограничило контроль за оборотом последних со стороны правоохранительных органов, что обусловлено программно-техническими особенностями. Возможность использования криптовалют в преступной деятельности связана с техническими особенностями технологии блокчейн, для которой характерны децентрализация эмиссии и оборота токенов, отсутствие рычагов регулирования, определенная степень анонимности.

В Республики Беларусь 21 декабря 2017 года вступил в силу Декрет Президента № 8 «О развитии цифровой экономики», который закрепил такие понятия, как виртуальный кошелек, криптовалюта, реестр блоков транзакций (блокчейн), цифровой знак (токен), а также явился определенной правовой базой использования криптовалют в Республике Беларусь[1].

Биткоин является наиболее распространенной криптовалютой, которая хранится на криптовалютных-адресах в криптовалютных-кошельках. Транзакции, в ходе которых осуществляется перемещение криптовалюты с одного адреса на другой, подписаны электронным образом и размещены в биткоин-сети, а также распространяются по всей сети криптовалюты, чтобы убедиться, что каждый участник осведомлен о них.

Изучение научной литературы и международного опыта показывает, что в преступных целях криптовалюта может использоваться для совершения киберпреступлений, отмывания и легализации преступных доходов; финансирования терроризма и экстремизма; совершения наркопреступлений и т. д. В силу специфики, присущей криптовалюте, заключающейся в отсутствии единого оператора, использовании криптографической защиты, определенной анонимности, возможности ее использования в преступной деятельности различны. Преступ-

[1] О развитии цифровой экономики: Декрет Президента Республики Беларусь 21 декабря 2017 г. № 8 // ЭТАЛОН. Законодательство Республики Беларусь. Минск, 2021.

никами также активно используются технологии дополнительной анонимизации (например, криптовалюта Монеро, технологии миксинга криптовалют).

При этом необходимо учитывать, что использование криптовалют не во всех случаях полностью анонимно. Базовым принципом блокчейна является прозрачность и публичность транзакций, что позволяет в определенной степени отследить цепочку операций участника сети, определить периодичность и объем переводов; установить адреса, с которых переводили суммы. Блокчейн биткоина не раскрывает никакой информации, которая могла бы привести к идентификации плательщика и получателя, однако изучение открытого исходного кода, информации, предоставляемой частным сектором, может приводить к идентификации интересующих лиц. С этой целью может использоваться информация, запрашиваемая на криптобиржах (контактные данные пользователей, IP-журналы, журналы активности, биткоин-адреса и адреса других криптовалют, используемые биткоин-пользователем для обмена валют, платежные данные и др.). Идентификация также возможна основе данных о криптокошельке и может реализовываться и транзакционный подход. С целью решения задачи по установлению пользователя по биткойн-адресам, в первую очередь, целесообразно использовать поисковые интернет-системы. Все биткоин-транзакции записываются в блокчейн – большую публичную базу данных, хранящую все данные в незашифрованном виде. Может представлять интерес информация из блокчейн-обозревателей[1] и иных ресурсов[2]. Отслеживание биткоин-потока с одного биткоин-адреса на другой не имеет смысла без характерной черты, связывающей хотя бы один из этих адресов с реальным субъектом.

Существуют коммерческие программные средства, которые можно использовать для анализа биткоин-транзакций и определения владельцев биткоин-адресов (Chainalysis, Elliptic, Blockseer, Ciphertrace, Bitanalysis), которые в определенной степени превосходят по своим возможностям инструменты с открытым исходным кодом, что обусловлено большим количеством идентифицированных объектов; возможностью экспорта данных; ссылками на биткоин-адреса и транзак-

[1] Blockchain // Blockchain.com – Mode of access. URL: https://www.blockchain.com/explorer.
[2] Endpoint Detection & Response (EDR). URL: https://encyclopedia.kaspersky.ru/glossary/edr-endpoint-detection-response.

ции из даркнета; графической визуализацией связей между кошельками.

В связи с активным использованием криптовалют для осуществления расчетов в компьютерной сети «Интернет» перспективным представляется совершенствование правового регулирования оборота криптовалют, с учетом их использования при совершении преступлений, а также совершенствование межгосударственного и международного сотрудничества по данному направлению по обмену опытом, взаимному оказанию правовой помощи, выявлению подозрительных операций с использованием криптовалюты, использованию технологий по деанонимизации участников преступных криптовалютных операций и т. д.

Отдельно следует остановиться на виктомологическом аспекте противодействия мошенничеству, совершаемому с использованием электронных средств платежа.

Поведение жертвы является составным элементом механизма преступления, поэтому одним из необходимых условий повышения эффективности предупреждения мошенничества в рассматриваемой сфере являются меры виктимологической профилактики, направленной на потенциальных жертв данного вида преступлений.

Основой данной деятельности является воздействие на виктимологические факторы, влияющие на совершение преступлений в сфере использования ЭСП. При этом следует учитывать как факт виктимности самих пользователей, так и компьютерных технологий и самих компьютеров – хранилищ информации. Поэтому к разработке мер виктимологической профилактики мошенничества должны привлекаться не только криминологи, но и технические специалисты.

Содержание виктимологической профилактики обусловлено несколькими аспектами. В организационном отношении виктимологическая профилактика имеет особенности, связанные со специальной подготовкой сотрудников правоохранительных органов. Недостаточность профессиональных знаний и практических умений не позволяют им своевременно осуществлять предупредительные мероприятия. Это обусловлено отсутствием в настоящее время приемлемых методических рекомендаций по организации и тактике виктимологической профилактики высокотехнологичных преступлений, конкретных методик работы с жертвами подобных преступлений.

В частности, определенные трудности вызывает проблема информационного обеспечения виктимологической профилактики мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий. Поэтому совместная работа правоохранительных органов со службами компьютерной безопасности, изготовителями антивирусных программных продуктов является залогом успеха виктимологической профилактики.

В качестве субъектов осуществления виктимологической профилактики мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий, выступают как государство в лице правоохранительных органов, так и общественные формирования, и иные негосударственные структуры. По своему объему виктимологическая профилактика данного вида преступлений охватывает различные формы поведения, являющиеся закономерным результатом разных вариантов виктимности: легкомысленность поведения, излишнее любопытство, пользовательская небрежность, незнание элементарных мер защиты, возрастные и интеллектуальные особенности и т. д. В качестве механизма регулирования виктимологической защиты выступают не только нормы права, но и морали, корпоративные и этические правила поведения.

В целом виктимологическая профилактика должна быть ориентирована на широкую социальную превенцию в целях минимизации высокотехнологичной преступности как общественно опасного явления.

Подводя итог вышеизложенному, представляется возможным сформулировать следующие выводы:

1) эффективность предупреждения мошенничеств данного вида во многом зависит от надежности программно-аппаратного обеспечения, используемого в организациях кредитно-финансовой сферы, способности систем безопасности противостоять компьютерным атакам, профессиональной подготовки сотрудников информационной безопасности и правоохранительных органов;

2) в контексте высокой общественной опасности мошенничества с использованием ЭСП стратегически важное значение приобретают современные технические (программно-технические) меры противодействия. Решения, лежащие в их основе, носят комплексный характер и сочетают в себе различные инструменты;

3) практическая реализация технических мер противодействия фишингу и фармингу базируется на ряде правил, в основе которых лежат антивирусная проверка подозрительных ссылок (URL) на предмет выявления вредоносного программного обеспечения, а также проверка whois – данных исследуемого сайта (домена); технические меры противодействия взлому сети, образующей «интернет вещей» пользователя, должны быть направлены в первую очередь на обеспечение защиты центрального компонента такой сети – Wi-Fi роутера;

4) меры противодействия мошенничеству в системах ДБО должны не только учитывать самые современные подходы к общепринятому программно-техническому обеспечению информационной безопасности, но и представлять собой взаимосвязанную систему мероприятий, направленных на обнаружение, предотвращение и пресечение действий злоумышленника;

5) противодействие мошенничеству с использованием ЭСП должно начинаться с эмиссионного банка и присутствовать на всех этапах финансовой транзакции.

Вопросы для самоконтроля

1. Определите понятие предупреждения мошенничеств, совершаемых с использованием электронных средств платежей.
2. Назовите субъектов предупреждения мошенничеств, совершаемых с использованием электронных средств платежей.
3. Назовите основные направления предупреждения мошенничеств, совершаемых с использованием электронных средств платежей.
4. В одном из районов города N участились случаи хищений с банковских счетов граждан. При этом злоумышленники используют «фишинговые» сайты для получения доступа к управлению счетами клиентов банка. Разработайте комплекс мер предупреждения названных преступлений.

Заключение

Мошенничество представляет собой угрозу, которая заслуживает серьезного внимания и требует безотлагательных действий со стороны государственных органов. Последствия мошенничества в рамках мировой российской экономики могут быть значительными. В дополнение к ощутимым финансовым потерям мошенничество влечет за собой пагубные последствия для репутации соответствующей кредитной организации, благосостояния общества в целом.

Следует отметить, что широкое применение таких новых форм безналичных расчетов, как расчеты с использованием банковских карт, а также использование возможностей последних достижений научно-технического прогресса на фоне ненадлежащего правового регулирования деятельности в банковской сфере привело к значительному росту преступлений.

Таким образом, наличие эффективных механизмов предупреждения и выявления мошенничества, и борьбы с ним имеет ключевое значение для защиты интересов общества и государства от негативных последствий в сфере использования электронных средств платежа.

Для эффективного противодействия мошенничествам необходима реализация комплекса профилактических мер, среди которых можно выделить следующие меры: повышающие трудность совершения преступлений; повышающие риск при совершении преступлений; уменьшающие выгоду от совершения преступления; направленные на повышение уровня цифровой финансовой грамотности всех участников; направленные на активное внедрение и совершенствование антифрод-систем; направленные на формирование в целом у граждан, а особенно в среде лиц, склонных к совершению киберпреступлений, убежденности в способности финансово-кредитного сектора и правоохранительных органов обеспечивать информационную безопасность; обеспечение передачи платежных данных только посредством защищенных каналов; переход части антифрод-сервисов на облачные технологии; реализация в системах-антифрод возможностей искусственного интеллекта, совершенствование правового регулирования осуществления платежей посредством использования криптовалют, в том числе разработка модельного законодательства.

Список использованных источников

1. О национальной платежной системе: Федеральный закон Российской Федерации от 27 июня 2011 г. № 161-ФЗ // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru.
2. О банках и банковской деятельности: Федеральный закон Российской Федерации от 2 декабря 1990 г. № 395-1 // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru.
3. Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru.
4. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // КонсультантПлюс: сайт. – URL: http://www.consultant.ru.
5. Анализ защищенности web-приложений. – URL: https://www.group-ib.ru/audit/web-apps.html.
6. Варламова С. Б. Оптимизация расчета величины операционного риска / С. Б. Варламова // Финансовые рынки и банки. – 2019. – № 1. – С. 36 – 44.
7. Данные судебной статистики // Судебный Департамент при Верховном Суде Российской Федерации: официальный сайт. – URL: http://www.cdep.ru/index.php?id=79.
8. Денисов Д. Актуальные вопросы противодействия мошенничеству в области электронных платежей / Д. Денисов // Банковский Вестник. – № 1. – 2014. – С. 61–64.
9. Дудников Е. А. Анализ существующих целей сетевых атак и способов атак на web-сервисы / Е. А. Дудников. – URL: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-tseley-setevyh-atak-i-sposobov-atak-na-web-servisy.
10. Зайцев О. Мошенничество в Интернете и защита от него / О. Зайцев / КомпьютерПресс: сайт. – URL: https://compress.ru/article.aspx?id=18184.
11. Зуйков Г. Г. Криминалистическое учение о способе совершения преступления: автореф. дис. ... д-ра юрид. наук / Г. Г. Зуйков.– М., 1970. – 31 с.

12. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра / С. В. Лебедь. – М.: МГТУ им. Н. Э. Баумана, 2002. – 306 с.

13. Лямин Л. Мошенничество в платежной сфере: Бизнес-энциклопедия / Л. Лямин, Н. Пятиизбянцев, А. Пухов. – М.: ЦИПСиР. – 2016. – 345 с.

14. Маркин Ю. В. Обзор современных инструментов анализа сетевого трафика / Ю. В. Маркин, А. С. Санаров. – URL: https://www.ispras.ru/preprints/docs/prep_27_2014.pdf.

15. О развитии цифровой экономики: Декрет Президента Республики Беларусь 21 декабря 2017 г. № 8 // ЭТАЛОН. Законодательство Республики Беларусь. – Минск, 2021.

16. Обзор рынка сетевых песочниц в России и мире. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Network - Sandbox#part2.

17. Олиндер Н. В. Криминалистическая характеристика электронных платежных средств и систем / Н. В. Олиндер // LEX RUSSICA (РУССКИЙ ЗАКОН). – 2015. – № 10. – С. 128–138.

18. Состояние преступности // Министерство внутренних дел Российской Федерации: официальный сайт. – URL: https://мвд.рф/folder/101762.

19. Что такое антифрод: задачи и методы. – URL: https://fisgroup.ru/blog/antifraud-zadachy-i-metody.

20. Blockchain // Blockchain.com – Mode of access. – URL: https://www.blockchain.com/explorer.

21. Endpoint Detection & Response (EDR). – URL: https://encyclopedia.kaspersky.ru/glossary/edr-endpoint-detection-response.

Содержание

Противодействие мошенничеству с использованием электронных средств платежа

Учебно-практическое пособие

Редактура *Г. Р. Кудояровой*
Компьютерная верстка *Д. Е. Звездиной*

Подписано в печать 29.12.2022. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 4,5. Уч.-изд. л. 4,5
Тираж 64 экз. Заказ № 84

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66