ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

НАУЧНО-КОНСУЛЬТАТИВНЫЙ СОВЕТ ПРИ СОВЕТЕ МИНИСТРОВ ВНУТРЕННИХ
ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

БЮРО ПО КООРДИНАЦИИ БОРЬБЫ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ
И ИНЫМИ ОПАСНЫМИ ВИДАМИ ПРЕСТУПЛЕНИЙ НА ТЕРРИТОРИИ
ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

НОВЫЕ СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ТЕРРИТОРИИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

АНАЛИТИЧЕСКИЙ ОБЗОР

МОСКВА 2018

УДК 34.343.9

Рекомендовано к опубликованию
редакционно-издательским советом ФГКУ «ВНИИ МВД России»

Р е ц е н з е н т ы:

В. А. Яковлев
(ДПД МВД России);
М. Ю. Воронин, доктор юридических наук, доцент
(Академия управления МВД России)

А в т о р ы :

И. Б. Колчевский, заместитель начальника НИЦ № 1 – начальник первого отдела, кандидат юридических наук, доцент;
В. М. Журавлев, старший научный сотрудник НИЦ № 2, кандидат юридических наук
(ФГКУ «ВНИИ МВД России»);
А. Г. Кузнецов, заместитель начальника Управления – начальник отдела содействия в межгосударственном розыске, экстрадиции, проведении специальных операций и координации борьбы с терроризмом, доктор социологических наук, профессор;
О. В. Демковец, старший инспектор по особым поручениям, кандидат юридических наук, доцент;
Д. А. Брехов, старший инспектор по особым поручениям
(БКБОП)

Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и О. В. Демковец, Д. А. Брехов. – М. : ФГКУ «ВНИИ МВД России», 2018. – 76 с.

Описываются новые способы совершения преступлений в сфере информационных технологий на территориях государств – участников СНГ в 2017 г.

Для сотрудников правоохранительных органов стран Содружества, слушателей образовательных организаций, а также представителей органов власти, уставных и рабочих органов государств – участников СНГ, занимающихся проблемами борьбы с преступностью в сфере информационных технологий.

УДК 34.343.9

ВВЕДЕНИЕ

В условиях устойчивого роста преступлений в сфере информационных технологий на территории государств – участников Содружества Независимых Государств[1] происходит консолидация усилий правоохранительных органов стран Содружества по ряду направлений международного взаимодействия. Одобрены и активно реализуются программа сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий на 2016-2020 годы; Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности от 10 октября 2008 года; Концепция сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 года; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года; Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года.

Вместе с тем в связи с появлением в настоящее время новых способов совершения преступлений в сфере информационных технологий ситуация в этой области такова, что приходится говорить о недостаточности принятых мер по противодействию этому виду современного криминала. Особенно остро обозначилась проблема распространения вредоносных компьютерных программ, представляющих угрозу государственным и транснациональным информационным ресурсам. Правоохранительные органы констатируют, что криминальные структуры активизируют попытки использовать открытые телекоммуникационные и ведомственные информационные сети для проведения крупных финансовых махинаций и мошеннических акций.

[1] Далее – СНГ, страны Содружества.

Особую тревогу правоохранительных органов стран Содружества вызывает практика использования информационных технологий террористическими организациями по приисканию и вербовке граждан, манипуляции массовым сознанием и распространению экстремистских взглядов.

Создаваемые уже сегодня сложные многослойные сети индустриального Интернета представляют собой связанные в единые системы различные типы программно-аппаратных платформ, которые могут быть как вертикальными, так и инфраструктурными, как основанными на использовании информационного пространства одного государства, так и нескольких, поэтому противодействие такого рода угрозам в рамках юрисдикции и возможностей сил и средств специализированных подразделений правоохранительных органов одного государства представляется затратным и малоэффективным, поскольку указанная преступная деятельность носит преимущественно транснациональный характер.

Все это обусловливает необходимость разработки механизма согласованных действий органов внутренних дел стран Содружества по борьбе с преступностью в сфере информационных технологий и актуализирует проведение комплексного научного анализа правовых и организационных аспектов данной проблемы в целях определения приоритетных направлений сотрудничества МВД (Полиции) государств – участников СНГ в данной области.

1. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ТЕРРИТОРИИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Интернет, став неотъемлемой частью жизни, вместе с тем часто используется для совершения правонарушений, направленных против личности, частной собственности, нравственных устоев и политического строя. Широкое использование в современной жизни компьютерных технологий и телекоммуникационных систем, создание на их основе глобальных компьютерных сетей привело к тому, что киберпространство стало активно использоваться для совершения преступлений. Результативность борьбы с этими угрозами обусловлена эффективностью применяемых государством правовых, организационных и кадровых мер в целом. Представляется целесообразным проанализировать на предмет наличия составов преступлений рассматриваемой направленности национальное уголовное законодательство государств – участников Содружества Независимых Государств.

Нормы уголовного законодательства **Азербайджанской Республики**, предусматривающие ответственность за совершение преступлений в сфере информационных технологий, содержатся в главе 30 «Киберпреступления» и включают следующие составы:

ст. 271. Неправомерный доступ к компьютерной системе;

ст. 272. Неправомерное завладение компьютерной информацией;

ст. 273. Неправомерное вмешательство в компьютерную систему или компьютерную информацию;

ст. 273-1. Оборот средств, изготовленных для совершения_киберпреступлений;

ст. 273-2. Фальсификация компьютерных данных.

Также Уголовный кодекс содержит норму в главе 23 «Преступления против собственности», относящуюся к преступлениям, совершенным с помощью информационных технологий: ч. 2.3-1 ст. 177 «Кража с использованием электронных носителей информации, либо

информационных технологий» (внедрена Законом Азербайджанской Республики от 30 апреля 2013 г. № 633-IVQD).

В МВД Азербайджанской Республики в составе Главного управления по борьбе с организованной преступностью функционирует управление по борьбе с киберпреступностью, фальшивыми деньгами и нелегальным оборотом фальшивых документов. Управление обрабатывает поступающую из разных источников информацию о киберпреступлениях, а также производит оперативно-технические мероприятия и регулярно проводит мониторинг сети Интернет в целях выявления и предотвращения таких видов преступлений.

По информации МВД Азербайджанской Республики, серьезных проблем правоприменительного и организационного характера в области борьбы с преступлениями в сфере высоких технологий в Республике не наблюдается. Поскольку уголовное законодательство Азербайджана содержит достаточно широкий перечень норм об ответственности за совершение такого рода деяний, новых способов совершения преступлений в сфере информационных технологий, их характерных особенностей, в том числе с использованием криптовалюты – биткоинов (Bitcoin)[2], не зарегистрировано.

Национальное законодательство **Республики Армения,** предусматривающее уголовную ответственность за совершение преступлений в сфере высоких технологий, содержит следующие составы:

ст. 181. Хищение, совершенное с использованием компьютерной техники;

ст. 226. Возбуждение национальной, расовой или религиозной вражды;

ст. 251. Несанкционированный доступ (проникновение) к системе компьютерной информации;

ст. 252. Изменение компьютерной информации;

ст. 253. Компьютерный саботаж;

ст. 254. Неправомерное завладение компьютерной информацией;

ст. 255. Изготовление или сбыт специальных средств неправомерного доступа (проникновения) к компьютерной информации;

ст. 256. Разработка, использование и распространение вредоносных программ;

[2] Более подробно о криптовалютах см.: Колчевский И.Б., Кузнецов А.Г., Брехов Д.А. Криптовалюты на территории стран Содружества: оценка вероятных криминальных рисков и угроз. М.: ФГКУ «ВНИИ МВД России», 2018.

ст. 257. Нарушение правил эксплуатации компьютерной системы или сети;

ст. 263. Незаконное распространение порнографических материалов или предметов.

По информации Полиции Республики Армения, в правоприменительной практике в сфере борьбы с киберпреступлениями отмечается наличие определенных трудностей, связанных с осуществлением оперативно-розыскной деятельности. Так, ст. 26 Закона «Об оперативно-розыскной деятельности» Республики Армения разрешает осуществлять мероприятия по контролю за телефонными разговорами, а также контроль за интернет-телекоммуникацией. На основании той же статьи осуществляется определение абонента телефонного номера либо владельца IP-адреса, которому на интересующий период он был предоставлен для интернет-доступа. Перечисленные оперативные мероприятия возможны только на основании решения суда и лишь в том случае, если санкция за преступное деяние предусматривает наказание в виде лишения свободы сроком свыше 5 лет. В Уголовном кодексе Республики Армения преступления такого типа причисляются к тяжким или особо тяжким преступлениям. Санкции в статьях, предусматривающих наказание за преступления в сфере высоких технологий, не превышают срок 5 лет. Зачастую это препятствует раскрытию уголовного дела на стадии дознания, а в ходе следствия следы преступления могут быть стерты.

В свою очередь органы следствия имеют право получить вышеуказанные данные на основании ст. 239 и 241 Уголовно-процессуального кодекса Республики Армения.

Существуют также определенные трудности, связанные с уголовно-процессуальным законодательством, в частности, сбор электронных доказательств, презервация интересующих данных, хранение данных интернет-сервис-провайдерами и т. д. Эти и другие пробелы в законодательстве учтены в проекте нового Уголовно-процессуального кодекса Республики Армения.

В качестве положительного примера раскрытия преступлений в рассматриваемой сфере следует отметить дело об организации и осуществлении компьютерных DDoS-атак[3] на ведущие букмекерские сайты Армении. В ходе предварительного следствия по данному

[3] DDoS – хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системам.

делу, в результате оперативного сотрудничества и взаимодействия Главного следственного управления по расследованию особо важных дел следственного комитета и отдела по киберпреступлениям при ГУБОП Полиции Республики Армения не только было раскрыто данное уголовное дело, но также были выявлены и другие преступные деяния, совершенные разными лицами, в том числе и лицами, находящимися за пределами Республики Армения.

По данным уголовного дела атаки производились хакерами, которые находились на территории Украины. В ходе расследования уголовного дела об организации компьютерного саботажа и незаконного присвоения компьютерных данных, совершенного группой лиц по предварительному сговору, установлены виновные, одно лицо объявлено в международный розыск. Ведутся также оперативно-розыскные мероприятия для выявления и привлечения к уголовной ответственности лиц, непосредственно осуществивших DDoS-атаки на сайты.

В структуре МВД **Республики Беларусь** с 2002 г. создано и функционирует подразделение, специализирующееся на профилактике и раскрытии преступлений в сфере высоких технологий, предусмотренных ст. 212 «Хищение путем использования компьютерной техники» и главой 31 «Преступления против информационной безопасности» Уголовного кодекса Республики Беларусь[4]:

ст. 349. Несанкционированный доступ к компьютерной информации;

ст. 350. Модификация компьютерной информации;

ст. 351. Компьютерный саботаж;

ст. 352. Неправомерное завладение компьютерной информацией;

ст. 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;

ст. 354. Разработка, использование либо распространение вредоносных программ;

ст. 355. Нарушение правил эксплуатации компьютерной системы или сети.

Вместе с тем практика показывает, что с использованием компьютерной и иной электронной техники совершаются и иные преступления. Наиболее встречающиеся упомянуты: в ст. 188 «Клевета», ст. 189 «Оскорбление», ст. 208 «Вымогательство», ст. 209 «Мошен-

[4] Далее – УК РБ.

ничество», менее распространенные: в ст. 145 «Доведение до самоубийства» и ст. 146 «Склонение к самоубийству».

В качестве примера можно привести выявление и раскрытие в 2016 г. ряда резонансных хищений с использованием компьютерной техники, распространения и использования поддельных банковских платежных карт, а также их реквизитов для осуществления хищений. Задержаны и привлечены к уголовной ответственности организаторы и активные участники международных организованных преступных групп, специализировавшихся на использовании «скиммеров» (2 группы), распространении реквизитов банковских платежных карт и хищении с их использованием денежных средств (1 группа), распространении «вирусов-блокировщиков» (4 группы). При этом необходимо отметить, что участники преступных групп, как правило, находятся за пределами Республики Беларусь.

Еще один пример, хищение денежных средств в особо крупном размере (527 тыс. долларов США, 67,5 тыс. евро и более 108 тыс. белорусских рублей), обнаруженное сотрудниками ЗАО «Альфа-Банк» в августе 2016 г. при инкассации 27 банкоматов, находящихся в гг. Минске, Витебске и Могилеве. Преступники получили несанкционированный доступ к серверам банка, в том числе к серверу управления банкоматами, что дало возможность осуществить хищение. В результате проведения комплекса оперативно-розыскных мероприятий установлена причастность к хищению граждан Молдовы, России и Украины. 23 января 2017 г. возбуждено уголовное дело по признакам ч. 3 ст. 212 УК в отношении неустановленного гражданина, который в период времени с 12.32 по 14.15 1 ноября 2016 г. с IP-адреса 217.147.83.43 (территориальное расположение – Великобритания) и в период времени 10.14 по 11.09 10 ноября 2016 г. с IP-адреса 217.118.81.215 (территориальное расположение – Российская Федерация) осуществил вход посредством программного обеспечения «Radmin» в операционную систему ПЭВМ одного из банков, действующего на территории Республики Беларусь[5]. С целью получения полного контроля над вышеуказанной ПЭВМ неизвестное лицо с 1 ноября 2016 г. в 12.32 установило модифицированное программное обеспечение «RMS», а также 11 ноября 2016 г. в 08.35 выполнило установку вредоносной программы «Trojan-Spy.Win32.KeyLogger», позволяющей регистрировать и передавать злоумышленнику нажатия клавиш на клавиатуре, движения и нажа-

[5] Далее – Банк.

тия клавиш «мыши». Далее злоумышленник совершил несанкционированные операции по переводу с банковского счета Банка денежных средств на сумму 300 тыс. российских рублей, которые выданы 11 ноября 2016 г. в 15.23 в ПАО «САРОВБИЗНЕСБАНК» (г. Дзержинск, Нижегородская область Российской Федерации), а также в последующем осуществил перечисление 250 тыс. российских рублей, которые также выданы 14 ноября 2016 г. в 14.51 в вышеуказанном отделении банка. Кроме того, неустановленное лицо 14 ноября 2016 г. в период времени с 13.03 по 16.15 пыталось совершить аналогичное хищение денежных средств Банка на общую сумму 750 тыс. российских рублей, но не довело свой преступный умысел до конца по причинам блокирования операций сотрудником Управления внутреннего контроля Банка. И такие факты нарушения закона государства без физического нахождения преступника на его территории не единичны.

В работе органов внутренних дел Республики Беларусь выделяется ряд вопросов[6], связанных с различным толкованием норм уголовного закона в правоприменительной практике. Так, правовые нормы, устанавливающие ответственность за совершение преступлений, предусмотренных ст. 349-355 УК РБ, конкурируют с иными нормами законодательства, что влечет за собой отсутствие общей правоприменительной практики.

К примеру, по фактам блокирования компьютерной техники и требований выплаты штрафа от имени МВД за просмотр материалов порнографического содержания возбуждаются уголовные дела как по признакам ст. 209 УК РБ, так и по ст. 351, 354 УК РБ, аналогично по фактам несанкционированного доступа к учетным записям пользователей социальных сетей, сопряженным с хищением денежных средств лиц из списка контактов потерпевших, возбуждаются уголовные дела как по признакам ст. 209 УК РБ, так и по ст. 349 УК РБ.

Опыт работы органов внутренних дел Беларуси показывает, что в правоприменительной практике сформировалось два подхода к квалификации преступных деяний указанной категории: преступление совершено путем использования компьютерной техники (например, хищение, мошенничество, вымогательство), т. е. технические средства используются в качестве орудия совершения преступления; во втором случае – преступные деяния квалифицируют, выделяя два

[6] По информации МВД Республики Беларусь.

и более состава преступления, один из которых относится к категории преступлений в сфере высоких технологий (например, ст. 349 и 209 или 349 и 208 УК РБ).

В Уголовном кодексе **Республики Казахстан**[7] глава 7 «Уголовные правонарушения в сфере информатизации и связи» содержит следующие составы:

ст. 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций;

ст. 206. Неправомерные уничтожение или модификация информации;

ст. 207. Нарушение работы информационной системы или сетей телекоммуникаций;

ст. 208. Неправомерное завладение информацией;

ст. 209. Принуждение к передаче информации;

ст. 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов;

ст. 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа;

ст. 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели;

ст. 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.

Иные составы преступлений, совершаемых с использованием информационных технологий:

ст. 188. Кража;

ст. 190. Мошенничество;

ст. 174. Возбуждение социальной, национальной, родовой, расовой, сословной или религиозной розни;

ст. 256. Пропаганда терроризма или публичные призывы к совершению акта терроризма;

ст. 313. Незаконное распространение произведений, пропагандирующих культ жестокости и насилия (отдельный состав не предусмотрен);

ст. 274. Распространение заведомо ложной информации;

[7] Далее – УК РК.

ст. 297. Незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка либо сбыт наркотических средств, психотропных веществ, их аналогов (отдельный состав не предусмотрен);

ст. 311. Незаконное распространение порнографических материалов или предметов (отдельный состав не предусмотрен);

ст. 312. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера (отдельный состав не предусмотрен);

ст. 105. Доведение до самоубийства (отдельный состав, предусматривающий побуждение детей к суициду через Интернет, не предусмотрен).

В оперативно-служебной деятельности органов внутренних дел Казахстана фиксируются отдельные проблемы, связанные с использованием социальных сетей, которые служат площадкой для распространения противоправной информации (Facebook, Twitter, ВКонтакте, Одноклассники и т. д.) и мессенджеров для сотовых телефонов (WhatsApp, Viber, Line и т. д.), которые открыты для свободного пользования[8]. Так, на видеохостинге «Youtube.com» и мессенджере «WhatsApp» пользователями часто размещаются видеосюжеты противоправного содержания (сцены насилия, пытки, истязания, похищение людей, распространение ложной информации, что может повлечь за собой массовые волнения и т. д.). При этом распространители зачастую скрывают себя, регистрируя подложные страницы либо страницы блокируются или удаляются модератором.

Нередко поводом к обращению граждан в правоохранительные органы является опубликование оскорбительных комментариев, в том числе с содержанием признаков разжигания социальной, национальной, религиозной и иной вражды.

Указанные ресурсы находятся вне юрисдикции Республики Казахстан. Какая-либо информация об интересующих пользователях может быть получена только по запросу либо на основании международного следственного поручения.

Особую сложность представляет установление источника информации на Facebook, Twitter, WhatsApp, Viber,Youtube, которые находятся под юрисдикцией иностранных государств.

[8] По информации МВД Республики Казахстан.

В последнее время Казахстан принял ряд законодательных мер, направленных на борьбу с высокотехнологичными преступлениями, поэтому в настоящее время проблем, связанных с применением норм уголовного законодательства, не возникает, поскольку в УК РК (в ред. от 3 июля 2014 г.), рассматриваемые правонарушения включены в отдельную главу статей. Кроме того, отдельные квалифицирующие признаки, предусматривающие использование информационных технологий, сетей коммуникаций, включены в ряд других статей, тогда как в Уголовном кодексе старой редакции (от 16 июля 1997 г.) все составы преступлений в сфере информационных технологий были сосредоточены в одной статье – ст. 227 УК РК «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ», которая предусматривала ответственность за неправомерный доступ к охраняемой законом компьютерной информации.

В **Республике Молдова** преступления в сфере информационных технологий регулируются Уголовным кодексом в главе XI «Информационные преступления и преступления в области электросвязи», которая содержит следующие составы:

ст. 259. Несанкционированный доступ к компьютерной информации;

ст. 260. Неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов;

ст. 260.1. Неправомерный перехват передачи информационных данных;

ст. 260.2. Нарушение целостности информационных данных, содержащихся в информационной системе;

ст. 260.3. Воздействие на функционирование информационной системы;

ст. 260.4. Неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных;

ст. 260.5. Подлог информационных данных;

ст. 260.6. Информационное мошенничество;

ст. 261. Нарушение правил безопасности информационных систем;

ст. 261.1. Несанкционированный доступ к сетям и услугам электросвязи;

ст. 186. Кража;

ст. 189. Шантаж;
ст. 190. Мошенничество;
ст. 177. Нарушение неприкосновенности частной жизни;
ст. 178. Нарушение тайны переписки;
ст. 208.1. Детская порнография;
ст. 175. Развратные действия;
ст. 175.1. Контакты с детьми в сексуальных целях.

В Республике в ведении Центра по борьбе с информационными преступлениями не было на рассмотрении ни одного материала о заражении информационных систем вирусными программами, нацеленными на их преобразование в сети по производству различных видов виртуальных денег, таких как биткоин.

Вместе с тем одна из главных проблем, с которыми сталкивается Центр в части сотрудничества с государствами – участниками СНГ, – запоздалое поступление ответа о судебной помощи с их стороны[9].

Согласно мнению МВД Республики Молдова, национальное законодательство требует приведения в соответствие с современными реалиями системы противодействия высокотехнологичной преступности, поскольку сохраняются отдельные барьеры и недостатки нормативного порядка.

Так, в Уголовном кодексе Республики Молдова большинство информационных преступлений отнесены к категории преступлений средней тяжести, что не позволяет выполнять необходимые специальные розыскные мероприятия. Так, ст. 178 «Нарушение тайны переписки» не предусматривает уголовную ответственность за деяния, совершенные в отношении электронной переписки (сообщений), поскольку в соответствии с законодательством Молдовы о связи понятие «почтовые отправления» предусматривает только отправленное и полученное физическое имущество. При этом ст. 208.1 «Детская порнография» не инкриминирует умышленное получение доступа к детской порнографии посредством информационных технологий и связи, хотя это предусмотрено Лансаротской конвенцией[10].

Большинство преступлений, предусмотренных в главе XI Уголовного кодекса Республики Молдова, – преступления в области компьютерной информации и преступления в области электросвязи –

[9] По информации МВД Республики Молдова.

[10] См.: Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (CETS № 201): заключена 25 окт. 2007 г. в Лансароте (Канарские острова, Испания): вступила в силу 1 июля 2010 г.

имеют материальный состав и сводятся к нанесению ущерба, превышающего 100 тыс. леев (около 6 тыс. долларов США)[11].

В уголовно-процессуальном законодательстве Молдовы не урегулированы процедура «информационного обыска», предусмотренная действующей для Молдовы Будапештской конвенцией, и снятие копий с информационных данных (клонирование)[12].

В законодательстве Молдовы отсутствует специальная розыскная мера по перехвату информационных данных, и не предусмотрена мера по получению сообщений электронными средствами – текстовая переписка посредством информационных систем вне услуг телефонной связи и других электронных сообщений – от поставщиков услуг электронной почты, чата и т. д.

Также в Молдове национальное законодательство не регулирует защиту критических инфраструктур, в том числе информационных, которые по мере ускорения процесса информатизации становятся все важнее. Понятие «критических инфраструктур», а также жизненно важные субъекты, относимые к этой категории, не определены государством. Это существенно уязвимая точка при обеспечении бесперебойной и нормальной работы основных государственных учреждений и жизненно важных служб.

На нормативном уровне не предусмотрено исключение доступа через Интернет к детской порнографии и прочей информации, размещаемой в ходе преступной деятельности или использованной для совершения преступлений.

В Уголовном кодексе **Российской Федерации** нормы о преступлениях, совершенных в сфере информационных технологий, выделены в самостоятельную главу 28 «Преступления в сфере компьютерной информации»:

ст. 272. Неправомерный доступ к компьютерной информации;

ст. 273. Создание, использование и распространение вредоносных компьютерных программ;

ст. 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

ст. 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (введена Феде-

[11] См.: URL: https://pokur.su/mdl/usd/100000. 1 MDL=0,06$ (дата обращения: 02.02.2018).

[12] См.: Конвенция о преступности в сфере компьютерной информации (ETS; 185): заключена в Будапеште 23 нояб. 2001 г.

ральным законом от 26 июля 2017 г. № 194-ФЗ и вступает в силу с 1 января 2018 г.).

Национальное законодательство Российской Федерации также предусматривает уголовную ответственность за совершение преступлений, которые могут совершаться с использованием информационных технологий и содержатся:

в ст. 110. Доведение до самоубийства (в ред. Федерального закона от 29 июля 2017 г. № 248-ФЗ);

ст. 110.1. Склонение к совершению самоубийства или содействие совершению самоубийства (введена Федеральным законом от 7 июня 2017 г. № 120-ФЗ);

ст. 110.2. Организация деятельности, направленной на побуждение к совершению самоубийства (введена Федеральным законом от 7 июня 2017 г. № 120-ФЗ);

ч. 1 ст. 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;

ст. 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации (введена Федеральным законом от 7 дек. 2011 г. № 420-ФЗ);

ст. 146. Нарушение авторских и смежных прав;

ст. 151.2. Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (введена Федеральным законом от 7 июня 2017 г. № 120-ФЗ);

ст. 158. Кража;

ст. 159. Мошенничество;

ст. 159.3. Мошенничество с использованием платежных карт;

ст. 159.6. Мошенничество в сфере компьютерной информации;

ст. 165. Причинение имущественного ущерба путем обмана или злоупотребления доверием;

ст. 171.2. Незаконные организация и проведение азартных игр;

ст. 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;

ст. 228.1. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества;

ст. 242. Незаконные изготовление и оборот порнографических материалов или предметов;

ст. 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних;

ст. 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов;

ст. 280. Публичные призывы к осуществлению экстремистской деятельности;

ст. 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации;

ст. 282.1 Организация экстремистского сообщества;

ст. 282.2. Организация деятельности экстремистской организации;

ст. 282.3. Финансирование экстремистской организации.

В МВД России функционирует Управление «К» БСТМ (Бюро специальных технических мероприятий), основными направлениями деятельности которого являются: борьба с преступлениями в сфере компьютерной информации; пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет; борьба с незаконным оборотом радиоэлектронных и специальных технических средств; выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий; борьба с международными преступлениями в сфере информационных технологий; международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

По информации Главного управления по контролю за оборотом наркотиков МВД России[13] схемы бесконтактного сбыта создают объективные сложности выявления, документирования и доказывания наркопреступлений. Серьезную опасность представляют специализированные форумы, в том числе в социальных сетях, темы которых посвящены употреблению наркотиков. На них происходит наиболее интенсивный обмен опытом среди наркозависимых лиц о способах изготовления (производства), культивации, приема и местах приобретения наркотических средств, а также о правилах поведения в случае задержания сотрудниками правоохранительных органов.

Помимо использования анонимных ресурсов сети Интернет, торговые площадки в Даркнете, осуществляющие сбыт различных видов наркотиков на территории России, Беларуси, Украины и Казахстана,

[13] Далее – ГУНК МВД России.

поддерживают сделки и оплату исключительно с использованием биткоинов.

Установлено, что к компании по продвижению проекта «HYDRA» привлечены предлагающие услуги в интернет-рекламе неустановленные лица, использовавшие возможности различных сервисов, предоставляющих в аренду так называемые виртуальные абонентские телефонные номера, одними из которых являются sms-reg.com и sms-aktivate.ru. К рекламной компании по продвижению «HYDRA» привлечено множество «фрилансеров», предлагающих услуги в интернет-рекламе. Направленные запросы о предоставлении сведений о лицах, арендовавших виртуальные номера, указанные в обращениях граждан, администраторами ресурса проигнорированы[14]. ГУНК МВД России отмечает, что общественный резонанс, повлекший ряд публикаций и телесюжетов в СМИ, играет на руку организаторам, не только позволяя отслеживать и принимать во внимание информацию о методах противодействия со стороны правоохранительных органов, но и способствуя рекламе ресурса.

С целью противодействия наркопреступности ГУНК МВД России совместно с Роскомнадзором посредством мониторинга Интернет-пространства выявляется и пресекается работа значительного количества интернет-ресурсов, пропагандирующих наркопотребление и распространяющих наркосодержащие препараты, а также осуществляющих финансовые услуги, в том числе по выводу денег, полученных от нелегальной продажи наркотиков, за рубеж. Большая часть указанных ресурсов зарегистрирована на территории иностранных государств, что не позволяет в полной мере пресекать их работу и привлекать к ответственности организаторов наркобизнеса.

Текущее развитие государственного механизма ограничения доступа к данным сайтам отстает от развития технологий, позволяющих скрыть либо подменить адрес компьютера пользователя, с которого осуществляется вход в Интернет, обеспечивает беспрепятственный доступ к сайтам, внесенным в списки запрещенных на территории России. При этом наибольшая доля продаж наркотиков осуществляется через анонимные онлайновые рынки или «темную сеть».

За преступления в сфере информационных технологий в Уголовном кодексе **Республики Таджикистан** уголовная ответственность предусмотрена:

[14] По сведениям ГУНК МВД России.

ст. 298. Неправомерный доступ к компьютерной информации, сопровождающийся нарушением системы защиты;

ст. 303. Разработка, использование и распространение вредоносных программ;

ст. 304. Нарушение правил эксплуатации компьютерной системы или сети;

ст. 241.1. Изготовление и оборот порнографических материалов или предметов с изображениями несовершеннолетних, с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет);

ст. 302. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети;

ст. 179.1. Вовлечение в совершение преступлений террористического характера или иное содействие их совершению;

ст. 179.3. Публичные призывы к совершению преступлений террористического характера и (или) публичное оправдание террористической деятельности;

ст. 307. Публичные призывы к насильственному изменению конституционного строя Республики Таджикистан;

ст. 307.1. Публичные призывы к осуществлению экстремистской деятельности и публичное оправдание экстремизма;

ст. 307.4. Организация учебы или учебной группы религиозно-экстремистского характера;

ст. 311. Разглашение государственной тайны.

Уголовное законодательство Республики Таджикистан содержит достаточно стройную систему норм об ответственности за преступления против информационной безопасности и в сфере информационных технологий, что представляет собой прочную правовую базу противодействия высокотехнологичной преступности. Тем не менее в оперативно-служебной деятельности милиции Республики существует ряд правоприменительных проблем. Например, Республика очень остро ощущает нехватку специалистов для раскрытия преступлений в сфере информационных технологий[15]. Как показывает практика, сотрудники правоохранительных органов в некоторых случаях осуществляют излишнюю квалификацию деяний общеуголовной направленности по статьям, предусматривающим ответственность за преступления в области информационных технологий.

[15] По информации МВД Республики Таджикистан.

С ноября 2013 г. в Управлении по борьбе с организованной преступностью МВД Республики Таджикистан создан Отдел по борьбе с преступлениями в сфере информационной безопасности.

Национальное законодательство **Республики Узбекистан** предусматривает уголовную ответственность за следующие виды преступлений, совершенных в сфере информационных технологий:

п. «г» ч. 2 ст. 103. Доведение до самоубийства;

п. «в», ч. 2, ст. 103.1. Склонение к самоубийству;

п. «в», ч. 2, ст. 168. Мошенничество;

п. «б», ч. 3, ст. 169. Кража;

п. «г», ч. 3, ст. 244.1. Изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности и общественному порядку.

Также в Уголовном Кодексе Республики Узбекистан содержится отдельная глава «Преступления в сфере информационных технологий», предусматривающая уголовную ответственность по следующим видам преступлений:

ст. 278.1. Нарушение правил информатизации;

ст. 278.2. Незаконный (несанкционированный) доступ к компьютерной информации;

ст. 278.3. Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе;

ст. 278.4. Модификация компьютерной информации;

ст. 278.5. Компьютерный саботаж;

ст. 278.6. Создание, использование или распространение вредоносных программ.

По информации, представленной МВД Республики Узбекистан, мониторинг сети Интернет, в том числе мессенджера «Telegram», показывает, что группа лиц по каналам этого приложения организует продажу синтетических наркотических средств.

Например, был выявлен автобот «Tashke_bot» под названием «СПАЙС СКОРОСТЬ РЕГ», в котором пользователям мессенджера «Телеграмм» предлагаются цены (прайс) на несколько видов синтетических наркотических средств путем перенаправления на оператора «@OPERATORBRO». Посредством этого уточняется местонахождение заказчика и предлагается оплатить через электронную платежную систему «QIWI».

Вышеуказанная схема организации незаконного распространения наркотических средств усложняет установку личности организаторов, так как в данном способе распространения наркотических средств нет физического контакта (путем обусловленного места «закладок») между курьером и покупателем.

Проанализировав национальное уголовное законодательство стран Содружества в сфере ответственности за киберпреступления, можно сделать вывод о том, что оно характеризуется относительным разнообразием.

Вместе с тем в большинстве государств – участников СНГ оно соответствует заключенной в г. Будапеште 23 ноября 2001 г. Конвенции Совета Европы о преступности в сфере компьютерной информации и закрепляет следующие группы компьютерных преступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием компьютерных данных; правонарушения, связанные с нарушением авторского права и смежных прав; акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

Внесенные в последнее время изменения в указанные законодательства обусловлены появлением и тенденциями развития киберпреступности. Уголовное законодательство стран Содружества демонстрирует разделение на преступления в сфере информационных технологий и преступления, совершенные с помощью компьютерной техники.

Совершенствование информационных технологий и их проникновение во все сферы человеческой жизни ведет к возникновению новых форм преступных посягательств и криминализации новых деяний, а это, в свою очередь, – к необходимости выработки эффективных мер борьбы с ними.

2. ХАРАКТЕРИСТИКА НОВЫХ СПОСОБОВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационных технологий обусловило их применение в преступленной деятельности. Анализ оперативной обстановки по линии предупреждения выявления и пресечения компьютерных преступлений свидетельствует о наличии устойчивой тенденции к изменению видов преступлений в сферах компьютерной информации и электронной коммерции в сегментах сети Интернет. Основную долю компьютерных инцидентов, по данным Совета руководителей органов безопасности и специальных служб государств – участников СНГ (СОРБ), составляет распространение вредоносных программ, предназначенных для хищения учетных записей пользователей сети Интернет, и преступления, связанные с электронными платежными системами. В настоящее время на первый план вышли хищения денежных средств у клиентов крупных банков, использующих систему дистанционного банковского обслуживания.

Способы совершения мошеннических действий с использованием сети Интернет, средств подвижной связи и систем дистанционного банковского обслуживания

Способы совершения данных преступлений обусловлены особенностями предмета и средств их совершения; использованием в преступных целях установленного порядка осуществления банковских операций по переводу безналичных денежных средств, находящихся на счетах банковских платежных карт, с использованием средств мобильной связи, а также порядка оказания услуг подвижной (так называемой мобильной) связи операторами связи.

Мошеннические действия с использованием мобильных средств связи путем перевода денежных средств со счетов банковских карт потерпевших на счета третьих лиц в большинстве случаев совершаются в отношении держателей банковских карт и владельцев мобильных средств связи, подключенных к системе «Мобильный

банк», путем вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей.

Они могут совершаться и в отношении держателей банковских карт, не пользующихся такими мобильными средствами связи.

Наиболее распространенные способы завладения чужими денежными средствами, находящимися на счетах банковских карт потерпевших, с использованием мобильных средств связи анализ материалов судебной практики позволяет классифицировать следующим образом.

1. *Введение потерпевшего в заблуждение относительно целей совершения перевода денежных средств путем совершения ему телефонных звонков или направления СМС-сообщений.* Под воздействием заблуждения потерпевший по своей воле самостоятельно производит перевод денежных средств со своего счета на счета третьих лиц с использованием системы «Мобильный банкинг» через терминалы банков или иным способом.

1.1. Побуждение потерпевшего к совершению действий по переводу денежных средств со своего счета на счета третьих лиц путем сообщения ему по телефону или направлением СМС-сообщения ложных сведений о внезапно возникших у их близких родственников серьезных неприятностей и проблем, связанных с несчастными случаями, совершением дорожно-транспортного происшествия, причинением вреда здоровью третьих лиц, задержанием за хранение наркотических средств, совершением других преступлений либо с долговыми обязательствами, для незамедлительного решения которых срочно требуется определенная сумма денег.

При этом виновные осуществляют звонки или направляют СМС-сообщения потерпевшим по случайно подобранным абонентским номерам телефонов, как мобильных, так и стационарных, представляются от имени их родственников, друзей, знакомых или сотрудников правоохранительных органов, а также указывают абонентский номер телефона или номер банковской карты, на который следует осуществить перевод и сумму денежных средств, которую необходимо перечислить. Во многих случаях мошенничество данным способом совершают лица, отбывающие наказание в местах лишения свободы.

1.2. Уведомление потерпевшего по телефону, в основном путем рассылки СМС-сообщений, о выпавшем ему крупном призе при

розыгрыше лотереи и необходимости перевода определенной суммы денежных средств на указанный номер телефона или платежного средства в качестве налоговых или иных платежей как условия получения приза.

1.3. Направление потерпевшему посредством СМС-сообщений ложных уведомлений о зачислении на его банковский счет определенной суммы денег, а через определенное время новых сообщений об ошибочном зачислении этих сумм с просьбой возврата их посредством перевода на указанный номер телефона или банковской карты.

1.4. Осуществление звонков потерпевшим от имени оператора связи с предложением подключить новую услугу и набрать для этого под диктовку определенный код, который в действительности является комбинацией для перевода денежных средств со счета абонента на счет третьего лица.

1.5. Одним из наиболее распространенных способов является сообщение потерпевшему заведомо ложных сведений посредством телефонных звонков или путем направления им СМС-сообщений от имени банка о якобы возникших технических или иных проблемах, препятствующих дальнейшему использованию им своей банковской карты с предложением совершить для устранения данных препятствий определенные операции по банковскому счету через систему «Мобильный банк», если она подключена к номеру телефона, или через терминал банка. Совершение потерпевшим, введенным в заблуждение, данных операций приводит в действительности к переводу денежных средств со счета его банковской карты на счет третьего лица.

Такие действия производятся лицами, совершающими мошенничество, как правило, в два этапа и в основном следующими двумя способами.

Первый способ – ложное уведомление о блокировке банковской карты. Потерпевшему направляется ложное уведомление посредством СМС-сообщения от имени банка о временной блокировке банковской карты с предложением навести подробные справки по указанному в СМС-сообщении номеру телефона.

В случаях, когда потерпевший, позвонив по указанному номеру, пытается выяснить причину блокировки его банковской карты, лица, совершающие мошенничество, представившись представителем службы безопасности банка, как правило, не сообщая какого, объясняют причины блокировки карты произошедшими по случайности

сбоями в работе сервера банка, попытками посторонних лиц получить информацию о реквизитах банковской карты или о банковском счете либо иными надуманными причинами. Затем виновные, в зависимости от полученной от потерпевшего информации по его ответам на поставленные вопросы, предлагают совершить для разблокировки банковской карты определенные действия с банковской картой посредством системы «Мобильный банк», если она подключена к его телефону, либо через ближайший банкомат. При этом потерпевшему сообщается о необходимости совершения данных действий в течение ближайших часов, поскольку в противном случае якобы возникнет необходимость совершения операции замены карты, которая может затянуться на долгое время (месяц), в течение которого воспользоваться денежными средствами на карте будет невозможно.

В случае согласия потерпевшего на выполнение ложной операции разблокировки карты, он подходит к банкомату и, перезвонив по указанному ему номеру телефона, действуя под диктовку, вставляет свою банковскую карту в банкомат, набирает на нем код доступа к карте и сообщает остаток денежных средств на карте. Затем набирает под диктовку цифры, якобы код для разблокировки карты, а в действительности переводит денежные средства со своей карты на банковскую карту или на лицевые счета абонентских номеров сотовых операторов третьих лиц, либо тем самым к его телефону подключают услугу «Мобильный банк», позволяющую управлять счетом его банковской карты при помощи СМС-сообщений. При этом потерпевшему становится известно по полученным чекам банкомата об осуществлении им операции перевода денежных средств. Однако потерпевшего убеждают, обращая его внимание на надпись внизу чека, что переведенные им денежные средства зарезервированы и в течение нескольких часов будут возвращены обратно на его счет и предлагают не пользоваться картой до их поступления.

После этого лица, совершающие мошенничество, в течение нескольких часов переводят поступившие денежные средства на банковские счета других лиц либо на счета до востребования через системы денежных переводов, осуществляемых отдельными кредитными учреждениями. При этом денежные средства в банке получают лица, неосведомленные об истинном их происхождении, за денежное вознаграждение и далее передают их незнакомым им лицам.

Используемые мошенниками для рассылки СМС-сообщений, разговоров с потерпевшими и для перечисления денежных средств

абонентские номера операторов связи, как правило, оформляются ими на вымышленных лиц, а банковские карты, на которые перечисляются похищенные денежные средства, принадлежат, как правило, не имеющим к ним отношения лицам, которые по просьбе других лиц или по своей инициативе оформляют их на свое имя и передают за денежное вознаграждение малознакомым или вообще не знакомым лицам.

Второй способ – введение в заблуждение держателя банковской карты (владельца счета) относительно сущности операций. Лица, совершающие мошенничество, при первом телефонном разговоре с потерпевшим выясняют, что абонентский номер его телефона подключен к системе «Мобильный банк». Поводом к образованию доверительных отношений с потерпевшим может стать, например, то, что виновный представляется сотрудником службы социального обеспечения либо сотрудником банка, целью которого является перечисление дополнительной социальной выплаты и т. п.

Затем виновные предлагают потерпевшему посредством данной системы совершить для разблокировки банковской карты операции якобы по временному резервированию денежных средств, находящихся на его банковском счете, а в действительности по переводу их на счета третьих лиц. После этого потерпевший, введенный в заблуждение, переводит под диктовку денежные средства со своего счета на указанный ему счет банковской карты или абонентского номера, будучи уверенным, что переведенные им денежные средства в течение суток поступят обратно на его банковский счет.

Разновидностью этого способа является *использование социальной инженерии.* Социальная инженерия (англ. social engineering) – это способ совершения преступлений в сфере компьютерной информации с использованием комплекса приемов, не имеющих отношения к программно-аппаратным методам несанкционированного доступа, совершаемых с использованием познаний в области психологии. Криминальное использование техники социальной инженерии предполагает либо получение информации, необходимой для несанкционированного доступа, либо вынуждение потерпевшего совершить необходимые злоумышленнику действия[16].

Так, в июле 2016 г. задержан интернет-мошенник, который путем использования социальной инженерии похитил с банковского

[16] См.: URL: http://www.hackzone.ru/pub/view/id/3253/; https://www.protectimus.com/blog/ru-social-engineering/ (дата обращения: 18.11.2017).

счета жителя г. Петропавловска, Казахстан, деньги в сумме 8 млн тенге[17].

К разновидностям введения в заблуждение потерпевшего также следует отнести *перевод средств со счета потерпевшего посредством использования системы «смс-банкинг»*. Технология смс-банкинга (от англ. SMS Banking) – разновидность технологии дистанционного банковского обслуживания с использованием СМС-сообщений, в которой доступ к банковским счетам и операциям по банковским счетам предоставляется в любое время с использованием номера мобильного телефона клиента, предварительно зарегистрированного в банке. Эта технология, помимо пассивного смс-оповещения о проведенных операциях и состоянии счета, позволяет осуществлять «активное» смс-оповещение – отправку СМС-сообщений в ответ на получаемые от клиента смс-запросы, например, запрос баланса банковской карты или счета, мини-выписки или блокировки банковской карты, а также отправлять банку через сеть оператора подвижной связи команды на проведение операций с денежными средствами клиента банка-владельца сим-карты.

Виновные пользуются возможностью совершать операции по USSD-запросам[18]. Лица, совершающие мошенничество, могут попросить набрать USSD-команду или отправить смс на специализированный номер банка (например, 900 для Сбербанка) для совершения перевода. Поскольку функционал смс-банкинга существует у многих банков, а многие клиенты не знают о такой возможности, виновные пользуются его возможностями для совершения мошенничества[19].

2. Вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем блокирования абонентского номера потерпевшего, восстановления его на дубликат сим-карты и перечисления денежных средств с банковского счета потерпевшего по-

[17] По информации МВД Республики Казахстан.

[18] USSD (Unstructured Supplementary Service Data) – стандартный сервис в сетях GSM, позволяющий организовать интерактивное взаимодействие между абонентом сети и сервисным приложением в режиме передачи коротких сообщений. Основное направление использования USSD-сервиса – предоставление абонентам возможности получать дополнительную информацию от приложений и управлять этими приложениями. USSD работает на всех существующих телефонах стандарта GSM, за исключением самых ранних моделей 1998–1999 годов выпуска.

[19] См.: URL: https://iz.ru/658024/anastasiia-alekseevskikh/v-rossii-poiavilas-novaia-moshennicheskaia-skhema (дата обращения: 05.11.2017).

средством системы «Мобильный банк», перевод денежных средств с банковской карты потерпевшего на счета третьих лиц[20].

Так, Л. будучи осведомленным о порядке и правилах доступа к автоматизированной системе и возможности перевода с ее помощью денежных средств без использования банковской карты владельца счета, действуя незаконно, путем обмана, под предлогом перечисления денежных средств на счет владельца банковской карты получил идентификационные данные карты. Продолжая осуществлять свой преступный умысел, Л., находясь в офисе сети продаж, обратился к специалисту с требованием о замене сим-карты по причине утери прежней. Специалист произвел замену, выдав новую сим-карту, что повлекло за собой автоматическое вмешательство в функционирование средства хранения, обработки и передачи компьютерной информации, а именно сим-карты, в виде ее блокировки. Л. произвел посредством ввода и передачи компьютерной информации, содержащейся в СМС-сообщениях сотового телефона, в информационно-телекоммуникационной сети оператора сотовой связи перевод денежных средств[21].

В некоторых случаях для получения дубликата сим-карты, установленной в телефоне потерпевшего, мошенники вступают в сговор с представителями оператора связи, работающими в офисах продаж и обслуживания клиентов[22]. В отдельных случаях данные преступления совершаются представителями оператора связи самостоятельно[23].

Особенностью указанных способов совершения мошенничества является отсутствие непосредственного контакта лиц, их совершающих, с потерпевшими, поскольку последние вводятся в заблуждение и побуждаются к совершению определенных действий посредством средств дистанционной коммуникации. Данная особенность обусловливает возможность совершения таких преступлений в отношении потерпевших, проживающих или находящихся в любом месте на

---

[20] См.: Приговор Юргинского городского суда Кемеровской области от 9 апр. 2015 г. по делу № 1-5/2015. URL: http://soj.consultant.ru/cgi/online.cgi?req=doc;base=AOSB;n=2860033;#0 (дата обращения: 05.11.2017).

[21] См.: Приговор Дзержинского районного суда г. Оренбурга от 23 марта 2015 г. № 1-157/2015. ULR: http: // sudact.ru/regular/doc/bfjWZb4l№z58 (дата обращения: 13.06.2017).

[22] См.: Приговор Самарского районного суда города Самары от 3 авг. 2015 г. № 1-156/15 // СПС КонсультантПлюс.

[23] См.: Приговор Советского районного суда города Самары от 17 марта 2016 г. по делу № 1-106/2016 // СПС КонсультантПлюс.

территории страны или за ее пределами, независимо от места нахождения лиц, их совершающих.

2. *Использование найденного, похищенного, приобретенного либо случайно оказавшегося у виновного чужого телефонного аппарата с абонентским номером владельца, подключенного к услуге «Мобильный банк».* Данный способ совершения преступления основывается на использовании мошенниками того обстоятельства, что потерпевший, у которого телефонный аппарат по тем или иным причинам выбыл из владения (утерян, похищен, продан вместе с сим-картой), своевременно не обращается в банк с просьбой отключить от его абонентского номера услугу «Мобильный банк» либо сам передает свой телефонный аппарат другому лицу для временного пользования или оставляет его временно без присмотра. Виновные, обнаружив при пользовании телефоном, что тот подключен к указанной услуге, пользуясь данным обстоятельством, совершают хищение денежных средств, находящихся на банковском счете потерпевшего[24].

3. *Использование подключенного к услуге «Мобильный банк» абонентского номера, ранее принадлежавшего другому абоненту.* Данный способ совершения мошенничества заключается в использовании лицами, его совершающими, того обстоятельства, что потерпевший, осуществив замену абонентского номера своего телефона, подключенного к услуге «Мобильный банкинг», не предупредил об этом кредитную организацию, а его абонентский номер впоследствии был перерегистрирован оператором связи на имя другого лица. Обнаружив при пользовании телефоном с таким абонентским номером, что тот подключен к услуге «Мобильный банкинг», новый владелец номера, пользуясь этим, производит посредством указанной услуги перевод денежных средств потерпевшего на свой банковский счет или на счета третьего лица[25].

Так, Н. была осуждена за совершение преступлений, предусмотренных чч. 1 и 2 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Согласно приговору суда Н., получив на мобильный телефон электронное сообщение о доступном лимите де-

---

[24] См.: Приговор Черниговского районного суда Приморского края от 22 сент. 2015 г. № 1-159/2015; Приговор Индустриального районного суда города Хабаровска от 30 сент. 2015 г. по делу № 1-717/2015; Приговор Первореченского районного суда города Владивостока от 11 марта 2016 г. по делу № 1-187/2016 // СПС КонсультантПлюс.

[25] См.: Приговор судьи судебного участка № 2 железнодорожного района г. Воронежа по уголовному делу № 1-67/2014. URL: https://rospravosudie.com/; URL: http://www.sudrf.ru (дата обращения: 13.06.2017).

нежных средств на не принадлежащем ей банковском счете, открытом на имя Ш., имела умысел на хищение указанной суммы и, реализуя его, используя принадлежащий ей мобильный телефон и сим-карту, к которой была ошибочно подключена услуга Мобильного банка Сбербанка России, предоставляющая техническую возможность распоряжаться денежными средствами, находящимися на расчетном счету Ш., путем ввода компьютерной информации в форме электрических сигналов (СМС-сообщения на номер 900) посредством телекоммуникационной сети оператора сотовой связи похитила денежные средства, принадлежащие Ш.[26]

Необходимо обратить внимание на то, что в настоящее время отмечается некоторое видоизменение схем хищения денежных средств в системах дистанционного банковского обслуживания (ДБО). Злоумышленники адаптировались к возрастающему уровню безопасности банковских систем.

Например, российскими кредитными организациями в 2017 г. утверждены принципы «двухфакторной авторизации», предполагающей проведение операции по двум независимым каналам (аккаунт ДБО, звонок по телефону, СМС-подтверждение, код со скретч-карты[27] или чека, электронная подпись и др.)[28]. В ответ на эти меры представители российских ОПС начали использовать методы замены сим-карт легальных владельцев банковских счетов. Ранее указанные действия были характерны для мелкого мошенничества, однако в текущем году объектами преступных посягательств стали главные бухгалтеры и руководители крупных коммерческих предприятий. Объем похищенных денежных средств в таких случаях исчисляется миллионами рублей[29].

---

[26] См.: Приговор Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу № 1-82/2013 // СПС КонсультантПлюс.

[27] Скретч-карта (англ. scratch card) – карта из картона или пластика с нанесенной на ней под защитным непрозрачным и стирающимся слоем некой закрытой информацией, в данном случае – паролем (кодом).

[28] Двухфакторная авторизация или аутентификация – это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную защиту аккаунта от несанкционированного проникновения.

Первый рубеж защиты – вход в систему через логин и пароль, второй – подтверждение входа вводом специального кода, приходящего по СМС на зарегистрированный в системе дистанционного обслуживания и привязанный к пользовательским данным телефонный номер или по электронной почте на почтовый ящик клиента, зарегистрированный в клиентской базе банка. (См., напр.: URL: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272/ (дата обращения: 15.11.2017)).

[29] По информации СОРБ.

Способы совершения хищений посредством вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем подделки электронных средств идентификации платежей, использования идентификационных данных платежных карт

Несанкционированное вмешательство в платежные системы – одно из наиболее распространенных способов хищений денежных средств со счетов физических лиц в кредитных организациях на территории государств – участников СНГ. Так, объем и количество операций, совершенных на территории Российской Федерации и за ее пределами с использованием платежных карт, эмитированных кредитными организациями, постоянно увеличиваются. По данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) в 2016 г. с использованием платежных карт было совершено более 296,7 тыс. несанкционированных операций на общую сумму 1,08 млрд рублей. В 2016 г. в Банк России была представлена информация о 717 несанкционированных операциях со счетов юридических лиц на общую сумму 1,89 млрд рублей. Основную долю как по объему, так и в количественном выражении несанкционированных операций составляют CNP-транзакции (операции в сети Интернет)[30].

Использование платежных карт, эмитированных банками, вошло в обыденную жизнь, однако совершение хищений средств держателей таких карт становится достаточно распространенным преступлением.

Банковские карты выпускаются кредитными организациями. К ним относятся: расчетные (дебетовые) карты, кредитные карты и предоплаченные карты, держателями которых являются физические лица, в том числе уполномоченные юридическими лицами, индивидуальными предпринимателями[31]. В объем понятия «платежная карта» включается понятие «банковская карта»[32].

---

[30] См.: Обзор несанкционированных переводов денежных средств за 2016 год. М.: Центральный банк Российской Федерации, 2017.

[31] См.: Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24 дек. 2004 г. № 266-П // Вестник Банка России. 2005. № 17.

[32] См.: Тарасенко О.А., Хоменко Е.Г. Банковское право: учебник. М.: Проспект, 2012. С. 274.

Хищение денег физических и юридических лиц посредством так называемого карточного мошенничества подразделяют на основные виды:

1) операции без присутствия карты:

несанкционированный доступ (хакерский взлом) к хранилищам данных платежной информации;

хищения денежных средств путем получения реквизитов платежных карт (фишинг);

2) банкоматы или POS-терминалы накладок и других устройств, копирующих данные магнитной полосы и запоминающих ПИН-код держателя (скимминг) в целях подделки карт (создание их копий);

3) кража карт или использование утерянного пластика (Lost/Stolen). Одна из технологических разновидностей – траппинг («ливанская петля») – захват карты в картридере с помощью специальных устройств с надеждой на то, что клиент уйдет, не дождавшись ответа, а мошенник извлечет банковскую карту из банкомата[33].

1. Фишинг – получение реквизитов банковской карты и идентификаторов ее держателя в целях последующего осуществления банковских операций со счетом потерпевшего с использованием полученных данных.

Способы получения учетных данных держателей банковских карт (пароля, логина, номера и кода проверки подлинности карты и др.) различны, тем не менее они сводятся к обману потерпевшего или копированию компьютерной информации[34]. После завладения путем обмана или иным неправомерным способом учетными данными потерпевшего мошенники, как правило, представившись от имени потерпевшего, получают у операторов связи либо у уполномоченных представителей дубликат сим-карты потерпевшего и через систему «Мобильный банк» или «Интернет-банкинг» осуществляют перевод денежных средств, находящихся на банковском счете потерпевшего, на счета третьих лиц.

Основные способы фишинга.

1. Достаточно распространенным является получение путем обмана или иным неправомерным способом реквизитов банковской

[33] См: Хоменко Е.Г., Тарасенко О.А. Национальная платежная система Российской Федерации и ее элементы: монография. М.: Проспект, 2017 // СПС КонсультантПлюс (дата обращения: 05.11.2017).

[34] Получение доступа к мобильному банку держателей банковских карт, попытки выведать платежные данные по телефону получили название «фишинг» (См.: Гуркина Е. Как защищался пластик // Финанс. 2009. № 41. С. 37).

карты и идентификаторов ее держателя и последующее осуществление с использованием полученных данных и средств мобильной связи перевода денежных средств, находящихся на банковском счете потерпевшего, на счета третьих лиц.

Например, широко распространена рассылка потерпевшим СМС-сообщений от имени банка о блокировке банковской карты с указанием номера телефона для получения справок, при звонке по которому потерпевшим сообщается о произошедшем техническом сбое в работе компьютерной системы банка и предлагается для разблокировки или перерегистрации карты сообщить представителю банка номер и код карты либо пароли для ее использования.

Получение обманным путем идентификационных данных (номера и кода проверки подлинности) банковской карты нередко совершается мошенниками под предлогом необходимости этих сведений для осуществления перевода денежных средств на банковский счет потерпевшего, в частности, в качестве оплаты за товар, объявление о продаже которого им размещено в сети Интернет[35].

2. Получение учетных данных путем обмана потерпевшего в момент пользования последним платежной картой для осуществления операций через банкомат. Мошенники обращаются к неосведомленному потерпевшему и просят проверить с помощью его карты, находящейся в картоприемнике банкомата, работу раздела «Интернет-обслуживание», после чего тот, согласившись, под диктовку проводит операции, завершающиеся распечаткой чека, содержащей полную информацию о банковской карте потерпевшего, включая идентификатор и пароли для пользования системой «Интернет-банкинг», которым мошенники тайно завладевают[36].

3. Наиболее распространенным способом копирования компьютерной информации, содержащей сведения об учетных данных держателей банковских карт, является создание, распространение и использование вредоносных компьютерных программ, перенаправляющих потерпевших на сайты-двойники или иные сайты с вредоносной программой в сети Интернет, на которых происходит копирование идентификационных данных потерпевших. В случаях с торгово-сервисными предприятиями по карте пользователя могут быть про-

[35] См.: Приговор Советского районного суда г. Рязани от 31 марта 2016 г. по делу № 1-88/2016 // СПС КонсультантПлюс.

[36] См.: Приговор Майминского районного суда Республики Алтай от 28 мая 2014 г. по делу № 1-40/2014 // СПС КонсультантПлюс.

ведены мошеннические транзакции за неприобретаемые в действительности товары и услуги.

Данный способ именуется **фарминг** (англ. pharming) и представляет собой процедуру скрытного перенаправления жертвы на ложный IP-адрес. Осуществляется с помощью вредоносного программного обеспечения, которое «перебрасывает» пользователя с запрошенных страниц Интернета на их мошеннические копии. Для этого может использоваться навигационная структура (файл hosts, система доменных имен (DNS)). Не подозревая об обмане, жертва вводит на сайте запрашиваемые данные: номера счетов, пароли, ПИН-коды и другие идентификационные данные, тем самым передавая их в руки преступников[37].

Мошенники распространяют на компьютеры пользователей вредоносные программы, которые направлены на манипулирование файлом HOSTS или изменение информации DNS. Например, мошенники осуществляют массовую рассылку СМС-сообщений, в которых предлагается скачать музыкальные или иные клипы, либо направляют ложные уведомления, в том числе от имени банков, с предложением установить программу с сайта банка, ссылка на который приводится в сообщении, для повышения уровня защиты своих персональных данных[38]. Либо может направляться письмо от банка, в котором даны указания клиенту подтвердить правильность своих реквизитов на специальном веб-сайте из-за возникших проблем технического характера. Или, к примеру, сообщение, что клиент банка превысил максимально допустимую отсрочку платежа и его счет будет заблокирован, с просьбой для более подробного ознакомления открыть прикрепленные документы.

4. Удобным, с точки зрения получения информации, относящейся к персональным данным и данным о платежной карте потерпевшего, включая ее номер, срок действия, CVV/CVC-код[39], транслитеральное написание имени и фамилии владельца на карте, является **создание двойников сайтов** по продаже авиа- и железнодорожных билетов, а также двойников сайтов финансовых организаций. 44 %

[37] По материалам электронных ресурсов. URL: http://www.banki.ru/wikibank/farming/; ru.wikipedia.org; https://www.protectimus.com/blog/ru-social-engineering/ (дата обращения: 18.11.2017).

[38] См.: Приговор Миасского городского суда Челябинской области от 25 мая 2016 г. по делу № 1-304/2016 // СПС КонсультантПлюс.

[39] Трех- или четырехзначный код, предназначенный для проверки подлинности карты при платежах в Интернете.

мошеннических ресурсов, обнаруженных в российском сегменте Интернета с начала 2017 г., – лжебанки. 29 % приходятся на лжемикрофинансовые организации, 23 % – на сайты, продающие авиабилеты. С начала текущего года ФинЦЕРТ Банка России направил регистраторам данные о 481 ресурсе, которые необходимо заблокировать[40].

5. **«Обход» двухфакторной аутентификации в системах «Интернет-банкинга»** с помощью СМС, которая используется подавляющим большинством банков в системах дистанционного обслуживания клиентов, который осуществляется следующим образом:

мобильное устройство пользователя заражается банковским троянцем[41];

пользователь запускает подлинное банковское приложение на своем смартфоне;

троянец определяет, приложение какого банка используется, и перекрывает его интерфейс своим, показывая пользователю поддельный экран. Внешне поддельное приложение максимально похоже на настоящее;

на поддельном экране пользователь вводит свои логин и пароль;

троянец отправляет эти логин и пароль злоумышленникам. В результате последние получают возможность использовать эти данные для входа в банковское приложение;

злоумышленники инициализируют перевод некоторой суммы денег на свой счет;

на зараженный смартфон пользователя от системы дистанционного обслуживания приходит СМС с одноразовым паролем;

троянец перехватывает пароль из СМС и отправляет его злоумышленникам;

при этом на смартфоне СМС скрывается – пользователь не видит сообщение и ни о чем не подозревает, пока не проверит список транзакций;

---

[40] См.: URL: https://iz.ru/651634/pochti-polovina-moshennicheskikh-saitov-v-internete-lzhebanki (дата обращения: 05.11.2017).

[41] Эксперты Лаборатории Касперского выделяют три разных семейства банковских троянцев, распространенных в последнее время:

Asacub – троянец-шпион;

Acecard – троянец, способный перекрывать своими фишинговыми экранами приложения около 30 разных банков;

Banloader – кросс-платформенный троянец бразильского происхождения, способный запускаться как на компьютерах, так и на мобильных устройствах.

(См.: Электронный ресурс. URL: https://www.kaspersky.ru/blog/banking-trojans-bypass-2fa/11172/ (дата обращения: 03.09.2017)).

используя перехваченный одноразовый пароль, преступники подтверждают свою транзакцию и получают деньги на счет.

2. Траппинг (англ. – trapping) – способ, при котором мошенник в картридер терминала вставляет кусок пленки, надрезанный таким образом, что карта, попадая в прорезь, не возвращается обратно владельцу, а попадает в некий конверт, который впоследствии извлекается мошенником.

В момент, когда карта попадает в ловушку, злоумышленник оказывается рядом с потерпевшим и предлагает ему ввести повторно ПИН-код, мотивируя это тем, что с ним накануне произошла подобная ситуация и это помогло вернуть карту. После «неуспешных» вводов ПИН-кода карта не возвращается, и мошенник советует обратиться в банк. Когда потерпевший уходит, конверт вместе с картой извлекается мошенником из банкомата. В итоге у преступника оказывается карточка потерпевшего и информация о ее ПИН-коде[42].

Анализ правоприменительной практики и научной литературы не позволяет говорить о распространенности траппинга или «ливанской петли» как элемента объективной стороны мошенничества.

3. Скимминг предназначен для считывания данных и распознавания ПИН-кодов карт. Для этого мошенники устанавливают на банкоматы считывающие устройства – скиммеры.

На картридер устанавливают рамки с магнитной головкой, считывающей информацию с магнитной полосы и записывающую дампы карт на встроенную микросхему памяти и/или на клавиатуру приклеивают накладку, очень похожую на настоящую клавиатуру, которая запоминает нажатия клавиш и также записывает их на встроенную микросхему.

Как вариант, вместо клавиатуры на банкомат крепят миниатюрную видеокамеру, которая снимает руку, вводящую ПИН-код, и записывает в модуль памяти, либо передает его дистанционно на компьютер мошенника. Обычно, в случае дистанционной передачи, мошенник находится где-то неподалеку и принимает видеоданные при помощи ноутбука.

Одним из способов считывания данных карты является установка на картридер для входа в помещение банка (в случае расположения банкоматов в закрытых помещениях, открывающихся посредством считывания карты) скимминговую накладку и считывают ин-

[42] См.: URL: http://www.banki.ru/wikibank/trapping/ (дата обращения: 09.09.2017).

формацию с карт входящих клиентов. Также рядом с картридером может прикрепляться клавиатура для ввода ПИН-кода.

Через некоторое время мошенник снимает скиммер с банкомата, записывает дамп карты на любую карточку с магнитной полосой и, используя ПИН-код, полученный с клавиатуры либо видеокамеры, снимает наличные через другие банкоматы.

Считанные с карт дампы могут также использоваться для изготовления клонов карт. Если ПИН-код мошенникам не известен, покупки совершаются с использованием «белого пластика» в магазинах при сговоре с кассиром.

Мошенники нередко пересылают дампы карт для изготовления подделок и обналичивания в другие страны. Это делается с целью усложнения расследования и переноса ответственности за мошенничество на банки, поскольку при отсутствии в паспорте клиента отметки о пересечении границы, банк не может возложить вину за несанкционированную операцию на владельца карты.

Например, в 2011 г. в г. Петропавловске, Казахстан, в ходе проведения оперативно-розыскных мероприятий задержан гражданин Германии, который путем использования поддельных пластиковых платежных карт нанес ущерб АО «Цеснабанк» свыше 14 млн тенге.

В 2013 г. в г. Алматы задержаны две группы (граждане Болгарии и Румынии), которые прибыли в Казахстан для совершения краж с установкой скимминговых устройств (устройства кустарного производства, устанавливаемые на банкоматы для копирования информации с пластиковых карт держателей) на банкоматы (АО «Народный банк» и «Сбербанк»). Владельцам карточек причинен ущерб на сумму свыше 8 млн тенге.

В 2015 г. в г. Астане задержаны граждане Молдовы, которые с использованием скимминговых устройств похитили информацию с карточек 90 клиентов Народного банка. Владельцам карточек причинен ущерб на сумму свыше 9 млн тенге.

В марте 2016 г. задержан житель г. Актобе, который установил скимминговое устройство на банкомат Казкоммербанка и похитил информацию с пластиковых карточек 51 клиента[43].

Современное оборудование терминалов и банкоматов, как правило, не позволяет устанавливать скимминговые устройства либо уже содержит в своей конструкции устройства активного антискимминга, которое контролирует пространство перед банкоматом и поз-

[43] По информации МВД Республики Казахстан.

воляет моментально выявить несанкционированную установку на него посторонних устройств, а также выдает радиопомехи в области щели картоприемника, препятствующие работе посторонних электронных устройств[44]. Поэтому скимминг – достаточно сложный и затратный способ хищения, хотя, как показывает практика, для Казахстана выявление и пресечение хищений, совершаемых этим способом, остается актуальным. При этом в Молдове в 2016 г. отмечено снижение числа случаев применения скимминга[45].

Следует отметить, что анализ итогов правоприменительной практики стран Содружества в области противодействия высокотехнологичной преступности позволяет констатировать, что практически все способы совершения хищений, в частности мошенничества, путем использования электронных платежных средств актуальны для всех стран Содружества.

Достаточно распространенными являются **способы проведения банковских операций (переводов, обналичивания) посредством несанкционированного доступа («хакерского взлома») к хранилищам данных и иной банковской информации**. К таковым относятся следующие.

1. Хищения денежных средств путем доступа к идентификационным данным сотрудников кредитных организаций.

Установление непосредственного контроля над компьютерными системами жертвы являются распространенным способом совершения указанного вида преступлений. В таких случаях в зону риска попадают предприятия и организации, внутренняя сеть которых имеет точку доступа к Интернету. Обычно целью преступников становится сервер баз данных систем бухгалтерского учета с возможностью доступа, как из внутренней сети, так и из сети Интернет. Злоумышленники, подобрав пароли к системе и получив полный контроль над ней, могут осуществлять либо шифрование данных, либо похищение учетных данных. В данном случае оборудование жертвы на протяжении длительного времени может использоваться злоумышленниками в преступных целях без ведома жертвы (подбор паролей, рассылка нежелательных почтовых сообщений и т. п.).

Ряд хищений, совершенных путем неправомерного доступа к учетным записям бухгалтеров крупных организаций в 2012-2013 гг., был зафиксирован в Республике Казахстан. В 2017 г. в Казахстане

[44] См.: URL: http://www.chclub.ru/skimmingatm (дата обращения: 05.11.2017).
[45] По информации МВД Республики Молдова.

зарегистрированы случаи, когда хакеры получали доступ к учетной записи ответственных банковских сотрудников, после чего совершали крупные хищения денежных средств со счетов банка. Атаки на информационные системы банков совершены из зарубежных стран. Хакер с использованием логина банковского сотрудника завышал кредитный лимит на заранее выпущенных пластиковых картах банка. Наличность снималась в России и странах дальнего зарубежья (Бельгия, Испания, Тайвань и др.). В результате у банков похищены денежные средства на сумму свыше 3,5 млн долларов США[46].

2. Хищения и вымогательства денежных средств с помощью «банковских» вирусов.

Ввиду появления новых технологических решений по усовершенствованию работоспособности «бот-сетей»[47] большая часть преступных групп, работающих против банков и их клиентов, по сведениям СОРБ отказывается от стандартных методов при распространении своих троянов в пользу спам-рассылок с возможностью автоматического цикла (как у трояна Dyre)[48].

Вирус троян Dyre (Dyreza) – Trojan-Banker.Win32.Dyre – вредоносная программа, специализирующаяся на краже банковской информации. Троянец распространялся в период с 2014 по 2016 г. В отличие от других распространенных банковских троянцев, программа перенаправляет интересующий троянца трафик на свои собственные серверы[49]. Для распространения Dyre злоумышленники применяли ботнет Cutwail.

Нападение с использованием Dyre происходит следующим образом: на ПК жертвы отправляется спам-сообщение, которое содержит загрузчик Upatre, замаскированный под факс. После исполнения Upatre загружает новую модификацию трояна Dyre, которая в свою очередь загружает компьютерного червя, идентифицированного как WORM_MAILSPAM.XDP. Затем червь использует установленный на

---

[46] По информации МВД Республики Казахстан.

[47] Бот-сеть или ботнет (англ. «*botnet*» произошло от слов «*robot*» и «*network*») – компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DoS и DDoS-атаки).

[48] По информации СОРБ.

[49] См.: URL: https://threats.kaspersky.com/ru/threat/Trojan-Banker.Win32.Dyre/ (дата обращения: 12.11.2017).

скомпрометированных устройствах почтовый клиент Microsoft Outlook с целью рассылки спам-сообщений, к которым и прикреплен загрузчик Upatre. Червь отправляет спам-сообщения не контактам жертвы, а на адреса почты, полученные с сервера злоумышленников. По окончании рассылки писем червь самоудаляется.

За 2017 г. зафиксирован устойчивый рост количества преступлений, связанных с распространением «криптолокеров»[50]. Функциональность данного вредоносного программного обеспечения (ВПО) предполагает возможность зашифровки файлов ПЭВМ криптоустойчивым механизмом шифрования. Как правило, жертвами становятся юридические лица, государственные учреждения и производственные предприятия, сотрудникам которых от имени государственных органов власти и управления направляются различные уведомления с вложенным ВПО.

Участились случаи совершения хищений с использованием банковских троянов Dyre и Lurk, нацеленных как на российские, так и зарубежные финансовые учреждения. Результаты деятельности указанных вирусов активно освещаются в зарубежных средствах массовой информации, а их разработчиками являются преимущественно граждане государств – участников СНГ[51].

Вирус Lurk, как и Dyre, относится к классу троянских коней – вредоносных программ, которые осуществляют несанкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители этой категории не умеют создавать свои копии, не способны к самовоспроизведению.

Предназначен для ведения электронного шпионажа за пользователем (вводимые с клавиатуры данные, изображения экрана, список активных приложений и т. д.), похищает конфиденциальную информацию пользователей для доступа к системам онлайн-банкинга ряда крупных российских банков. Управляется удаленным командным сервером злоумышленника, куда передается найденная информация. Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы. По количеству атакованных пользователей Россия находится на первом месте[52].

---

[50] Программы-«криптолокеры» используются для вымогательства денежных средств за расшифровку файлов на ПЭВМ жертвы.

[51] По информации СОРБ.

[52] См.: URL: https://threats.kaspersky.com/ru/threat/Trojan-Spy.Win32.Lurk (дата обращения: 12.11.2017).

С целью сокрытия следов своей противоправной деятельности злоумышленниками активно используются средства анонимизации («VPN», «TOR», «Ргоху»), шифрования интернет-трафика, компьютерной техники и личной переписки, а также используются серверы, неподконтрольные российским правоохранительным органам. Из-за наличия «сервисов», предоставляющих услуги по обналичиванию денежных средств, отслеживание движения похищенных денежных средств в большинстве случаев не представляется возможным.

Необходимо отметить, что сегодня большое распространение получили программы malware типа RANSOMWARE. Ransomware или трояны-вымогатели (от англ. ransom – выкуп и software –программное обеспечение) – вредоносное программное обеспечение, предназначенное для вымогательства. Их можно разделить на два основных типа – шифровальщики (крипторы, cryptoransomware) и блокировщики (blockers, блокеры). Шифровальщики, попадая в компьютер, шифруют ценные файлы: документы, фотографии, базы данных и т.п. таким образом, что их нельзя открыть. За расшифровку создатели шифровальщиков требуют выкуп (в среднем около 300 долларов США).

В последнее время отмечается рост разнообразия и распространения RANSOMWARE. В мае 2017 г. вымогатель WannaCry поразил сотни тысяч компьютеров по всему миру. От атак вымогателя пострадали не только простые пользователи, но и многочисленные компании и организации. Распространение вируса было успешно остановлено. Вирус Petya был обнаружен в начале 2016 г. Но сегодня по состоянию на июнь 2017 г. из разных стран поступают сообщения о массовых заражениях «Петей» организаций и пользователей Украины, Великобритании, Индии, Голландии, Испании, Дании и др. Блокировщик-шифратор Mischa в качестве выкупа требует почти 2 биткоина (1,93), что составляет примерно 875 долларов США[53].

В июле-августе 2016 г. в Республике Молдова усилилось заражение информационных систем RANSOMWARE, замаскированным под полицейское приложение. Malware ведет к блокированию экрана мобильного телефона, а также компьютера, с вымогательством определенной денежной суммы под предлогом уплаты штрафа за правонарушение в правоохранительные учреждения.

[53] См.: URL: https://xakep.ru/2017/06/27/petya-outbreak/; https://www.kaspersky.ru/blog/ransomware-for-dummies/13579/; http://ru-wiki.org/wiki/Ransomware (дата обращения: 19.11.2017).

Сразу же после заражения системы, malware блокирует информационную систему и выводит на экран сообщение «от имени» Министерства внутренних дел. В этом случае жертву предупреждают, что у нее якобы имеются незаконные файлы, которые были выявлены после сканирования компьютера, или что она якобы просматривала запрещенные сайты. Кроме того, от пользователя требуют заплатить «штраф» через онлайновую платежную систему.

Malware прикреплен к веб-сайтам порнографического содержания, это самые зараженные категории сайтов. По имеющейся информации, malware появляется на 25 % сайтов с видео- или аудиосодержанием, (веб-страницы порнографического содержания); еще 21,63 % относятся к программам типа «installer» (программы, предназначенные для установки на драйверах, плагинах и т. д.) или программным update-ам; 16,53 % выдавали себя за программы «сгаск» и генерирующие ключи; еще 16 % были URL для социальных сетей[54].

В Беларуси также фиксируются факты блокирования доступа к информации под предлогом оплаты штрафов за какие-либо противоправные деяния. В таких случаях жертва осуществляет переход по выглядящей легитимно ссылке и попадает на страницу, содержащую специальную подпрограмму (скрипт) и блокирующую работу браузера посредством вывода специального окна (баннера), содержащего надпись о нарушении норм законодательства и необходимости оплаты штрафа как условия снятия блокировки. Как правило, блокировка доступа в указанных случаях не является фатальной и позволяет решить проблему с использованием перезагрузки устройства[55].

Иные способы хищений и причинения имущественного ущерба посредством использования средств подвижной связи

Данные способы не связаны с проникновением в компьютерные системы или операционные системы телефонов, они, скорее, должны быть связаны с приемами социальной инженерии.

1. Взимание повышенных сборов за телефонные звонки – одно из преступных явлений в области информационных технологий, которое актуально для Молдовы и заключается в повторяющихся случаях присвоения обманным путем денежных средств клиентов компаний

[54] По информации МВД Республики Молдова.
[55] По информации МВД Республики Беларусь.

телефонной связи, совершающих звонки на зарубежные телефонные номера, за которые взимается повышенный сбор.

Мошенническая схема состоит в «сброшенных» звонках преступников на номер телефона жертвы. Потерпевший, желая узнать, кто ему звонил, осуществляет звонок по соответствующему номеру телефона. Лица, сами того не зная, заплатят за сделанный телефонный звонок по завышенной цене на «платный номер».

К этому способу следует отнести схему мошенничества, когда виновные отправляют потерпевшему текстовое сообщение с незнакомого номера. Если лица отвечают на СМС из любопытства, с них снимается плата по специальному тарифу за СМС-сообщение.

2. Мошенничество на платформах бесплатных объявлений.

Для Молдовы актуальна мошенническая схема, состоящая в размещении бесплатных объявлений в Интернете о продаже различных видов продукции по цене, в несколько раз ниже цены аналогичных предложений на рынке, что привлекает внимание большого количества людей, заниженная цена объясняется собственником товаров срочной потребностью в денежных суммах, а выставленный на продажу товар не имеет никаких технических или внешних недостатков.

В контактной информации мошенники указывают контактные данные, которые фактически недоступны, объясняя это тем, что они находятся за пределами Республики Молдова, тут же предлагаются и альтернативные контактные данные, адрес электронного почтового ящика, имена профилей мгновенных сообщений, таких как Skype, ICQ, Messenger и т. д.

Во время переговоров, которые ведутся посредством альтернативных контактов, преступники просят перечислить денежные суммы в качестве аванса через различные международные системы денежных переводов под предлогом подтверждения реальных намерений покупателя. Однако в некоторых случаях преступники просят такими способами совершить дополнительные платежи, ссылаясь на различные надуманные причины (ремонт выставленного на продажу объекта, отсутствие денег на счете мобильного телефона и т. д.). Завладев деньгами, преступники прекращают любые контакты с жертвой[56].

3. Мошенничество в виде конкурса СМС или конкурса на общие знания состоит, как правило, в текстовом сообщении и может призывать жертву поучаствовать в конкурсе на получение ценного приза. Также сообщение (или иногда реклама) может приглашать к участию

[56] По информации МВД Республики Молдова.

в конкурсе на общие знания, где разыгрывается крупный приз, если они верно ответят на определенное количество вопросов. Мошенники изымают у потерпевших деньги посредством установления крайне высоких тарифов на сообщения, которые будут отправляться жертвами, и любые другие сообщения, которые будут ими получены. В случае мошенничества в виде конкурса на общие знания, первый набор вопросов устанавливается очень легким, чтобы поощрить потерпевших к продолжению игры. Между тем на последний вопрос или на последние два вопроса, на которые необходимо ответить, чтобы завоевать «приз», очень сложно или даже невозможно ответить верно[57].

Использование информационных технологий для совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров[58]

Компьютерные сети и телекоммуникационные технологии весьма широко используются в сфере незаконного оборота наркотических средств. Организованные группы наркоторговцев все чаще прибегают к бесконтактным способам сбыта наркотиков, широко используя при этом средства мобильной связи, интернет-ресурсы, электронные платежные системы. Отмечается нарастающее распространение применения бесконтактного способа сбыта наркотиков с распространением наркотиков посредством интернет-торговли.

В первом полугодии 2017 г. ГУНК МВД России совместно с территориальными подразделениями наркоконтроля выявлено 3 775 преступлений, связанных с незаконным оборотом наркотиков (прежде всего синтетических), совершенных с использованием интернет-технологий, возбуждены уголовные дела в отношении 1 583 лиц, причастных к их совершению, из незаконного оборота изъято свыше 760 кг наркотиков[59].

Одной из тенденций последнего времени является активизация нелегального производства синтетических наркотиков на территории стран Содружества, что определяется их доступностью по цене и способу приобретения, в том числе через сеть Интернет. Например, организацию в России подпольных лабораторий по преобразованию «концентратов» в готовые к потреблению вещества определяет уве-

[57] Там же.
[58] Далее – наркотики, наркотические средства.
[59] По сведениям ГУНК МВД России.

личение поставок крупных партий синтетических наркотиков («концентратов») с территорий государств Азиатского региона, в основном из Китая. В настоящее время фиксируется рост незаконного оборота новых психоактивных веществ, схожих по своему воздействию на организм человека с такими наркотическими средствами, как амфетамин, марихуана и ЛСД, что обусловлено практически неограниченными возможностями их синтеза, производства, а также низкой стоимостью.

Для транспортировки наркотиков активно используются каналы международной почтовой связи, ввиду отсутствия первичного контроля за вложениями в почтовые отправления и проверки документов отправителя. Выявление наркотиков в потоке грузов и почтовых отправлений возможно лишь при наличии оперативной информации о конкретной поставке.

Основным способом распространения наркотиков является бесконтактный сбыт путем организации тайников-закладок и переводом денежных средств через различные платежные системы, в том числе криптовалюты. С целью увеличения числа наркопотребителей участники наркобизнеса все активнее используют сеть Интернет не только в целях рекламы наркотических средств и психотропных веществ, но и в целях анонимного осуществления оперативного поиска продавцов и покупателей, организации так называемого «регионального маркетинга».

В целях организации торговли наркотиками активно используются ресурсы «темной сети» (DarkNet) или «глубокой паутины» (DeepWeb), которая обеспечивает анонимность, она закрыта от поисковиков и отслеживания. Попасть в DarkNet можно через один из прокси-серверов, самый популярный из которых – сеть Tor и ее браузер Tor (The Onion Router) Browser. Сайты сети Tor имеют доменное имя первого уровня onion.

Сайты наркоторговцев устроены по принципу обычных интернет-магазинов – в них можно оформить заказ, почитать отзывы и описание, поделиться мнением о качестве продукта и сервиса, связаться со службой поддержки. Оплата покупок возможна любыми способами, как банковскими картами, так и через интернет-кошельки либо криптовалютой, например, биткоинами.

DarkNet также используется организаторами и подстрекателями создания преступных групп для вовлечения в свою деятельность распространителей, т. е. осуществляется так называемое трудоустрой-

ство. В Даркнете предлагаются «вакансии» кладменов, которые делают закладки наркотиков; гроверов, которые выращивают траву; химиков, которые «варят» ЛСД и экстази; курьеров, которые перевозят товар; дропов, которые снимают деньги; и трафаретчиков, которые пишут объявления на асфальте и заборах. Требования к таким соучастникам незаконного оборота наркотиков – активность и профессионализм. Предлагается высокая зарплата и частичная занятость.

Самым крупным тематическим Интернет-форумом является Legal.RC, посредством которого также осуществляется торговля наркотиками через специальные ветки Интернет-магазинов.

С 2014 г. в русском сегменте Даркнета действует система моментальных магазинов, автошопов, которые позволяют приобрести дозу наркотика практически мгновенно – сразу после оплаты клиенту «скидывают» адрес ближайшей к нему закладки с нужным веществом. В сети Интернет распространены сайты «автопродаж» (например, ayerc.biz, shamarc.biz, uralklad.biz, xxx24.biz, Buddabar.biz, «parfumer22», «Staff-store», «Адреналин», «Антибиотик», «Ice-Team», «Хип Хоп Алеся», «Marvel», «Niko_TM64», «Big Russian Boss» и мн. др.), доступ к которым осуществляется как напрямую, так и через сервисы обмена мгновенными сообщениями, а также с применением так называемых виртуальных абонентских телефонных номеров, одними из которых являются sms-reg.com и sms-aktivate.ru.

Например, в 2016 г. УБН ДВД Павлодарской области, Республика Казахстан, выявлено два сайта (bratan01.biz и bratan01.net), на которых распространялись наркотические и психотропные вещества. В ходе проведенных следственно-оперативных мероприятий за распространение психотропных веществ задержаны и привлечены к уголовной ответственности 2 лица[60].

К настоящему времени ГУНК МВД России выявлено 1 345 интернет-ресурсов, через которые в России распространяются наркотики. Решением Роскомнадзора доступ к ним запрещен, однако подавляющее их число размещено на зарубежных серверах, не доступных для полной блокировки. Существует возможность посещения подобных интернет-ресурсов через различные программы свободного доступа, например, TOR или VPN-сервисы.

С 2014 г. в русскоязычном сегменте TOR организована и в настоящее время активно развивается торговая площадка «Ramp (Russian Anonymous Marketplace)», на которой размещена реклама 33

[60] По информации МВД Республики Казахстан.

оптовых и 121 розничного магазинов. На данной площадке преимущественно осуществляется сбыт традиционных видов наркотиков, таких как кокаин, гашиш, марихуана, амфетамин и МДМА. В персональном разделе одного из крупнейших оптовых магазинов, расположенных на «Ramp», «Sadovnik Shop» (пятый в рейтинге магазинов) размещены объявления региональных дилеров, расположенных в ряде городов России, а также на территории Республик Беларусь и Казахстан. В результате проведения комплекса оперативно-розыскных мероприятий, направленных на пресечение деятельности участников «Sadovnik Shop», из незаконного оборота изъято: 16,9 кг гашиша, 6,1 кг марихуаны, 56,9 кг амфетамина, 630 г кокаина, 3,2 кг МДМА.

С целью сбыта наркотиков преступники организовали структурные подразделения в регионах Российской Федерации, наладили логистическую цепочку, включающую в себя доставку особо крупных партий наркотических средств «курьерами» в места скрытого хранения и дальнейшую их передачу посредством «тайников-закладок». Связь между членами наркогруппировки осуществлялась посредством мессенджера «Telegram», расчеты производились с использованием различных криптовалют и электронных платежных систем.

Так, с конца октября 2016 г. неустановленными лицами, предположительно также являющимися организаторами «Legalrc» и «Way a Way», создана торговая площадка «HYDRA». В настоящее время на торговой площадке представлено более 400 магазинов, осуществляющих сбыт различных видов наркотиков на территории России, Беларуси, Украины и Казахстана. Структура TOR-сайта схожа с аналогичными ресурсами, действующими в ЕС и США. Сделки и оплата исключительно с использованием биткоинов происходят непосредственно на площадке. Установлено, что к компании по продвижению проекта «HYDRA» привлечены предлагающие услуги в интернет-рекламе неустановленные лица, использовавшие возможности различных сервисов, предоставляющих в аренду так называемые виртуальные абонентские телефонные номера, одними из которых являются sms-reg.com и sms-aktivate.ru. К рекламной компании по продвижению «HYDRA» привлечено множество «фрилансеров», предлагающих услуги в интернет-рекламе. Направленные запросы о предоставлении сведений о лицах, арендовавших виртуальные номера, указанные в обращениях граждан, администраторами ресурса проигнорированы[61].

[61] По сведениям ГУНК МВД России.

Кроме того, для организации СПАМ-рассылок с рекламой указанных магазинов и способов обхода блокировки используются программы-мессенджеры. Указанные в объявлениях электронные кошельки и почтовые адреса, номера телефонов и пр. оформляются на вымышленных лиц или по поддельным документам. Используемые номера абонентов сотовой сети, как правило, являются виртуальными и не имеют «привязки» к физическому лицу, и соответственно проведение оперативно-технических мероприятий по ним невозможно.

Использование информационных технологий с целью совершения преступлений против половой неприкосновенности несовершеннолетних, а также преступлений против здоровья населения и общественной нравственности

С развитием научно-технического прогресса Интернет становится все более востребованным и популярным среди детей и подростков. Растет количество времени, проводимого несовершеннолетними в Сети, увеличивается интенсивность ее использования. Нахождение онлайн становится вполне привычным, обыденным способом существования.

Сетевые технологии в настоящее время применяются в производстве и распространении детской порнографии. В последнее время отмечено частое использование сетей по распределению файлов, позволяющих осуществлять быстрый обмен изображениями и видеозаписями из разряда детской порнографии, без использования центральных серверов данных или Веб-сети, избегая тем самым регистрации поставщиками услуг данных о пользователях, которые могут стать доказательствами в ходе возбужденных уголовных дел[62].

Одно из наиболее востребованных направлений использования Интернета – социальные сети, которые дают возможность несовершеннолетним общаться и обмениваться информацией со своими друзьями. В России более 75 % детей имеют профиль в социальных сетях, при этом почти треть имеют больше одного профиля в разных сетях. Лидером популярности среди них выступает «ВКонтакте» – 89 %, далее следуют «Одноклассники» – 16 %, «Facebook» – 4 %,

[62] По информации МВД Республики Молдова.

«Myspace» – 2 %. Почти каждый пятый (19 %) российский ребенок имеет более 100 виртуальных друзей[63].

Находясь в виртуальном пространстве, дети и подростки неизбежно сталкиваются с комплексом киберугроз. Одной из наиболее опасных выступает угроза стать жертвой преступления против половой неприкосновенности, так как преступники, используя информационные технологии, получают возможность дистанционно связываться с детьми и подростками, осуществлять в их отношении развратные действия: демонстрировать материалы эротического и порнографического содержания; свои половые органы; мастурбировать; осуществлять разговоры на эротические темы и многое другое.

По мнению экспертов, в современных условиях практически от 70 до 100 % порнографических изображений несовершеннолетних распространяется с помощью сети Интернет. Теневой виртуальный рынок оборота детской порнографии успешно развивается. В сети спрос на детскую порнографию в 3–5 раз превышает предложения, а рынок потребления захватывает в основном страны Европейского Союза и США. Согласно опубликованным данным Европарламента, более 40 % несовершеннолетних пользователей сети Интернет уже сталкивались со случаями онлайновых обращений к ним взрослых лиц, просивших о личной встрече или виртуальном общении с помощью установленной на компьютере веб-камеры, более половины из них откликнулись на подобные предложения. При этом порнографические материалы с изображениями несовершеннолетних, изготавливаемые на территории России, с огромной прибылью распространяются через Интернет к конечным пользователям – жителям стран Европы и США, а также «домашним» потребителям[64].

Например, 30-летний житель Екатеринбурга М. осужден за совершение преступления, предусмотренного ч. 2 ст. 135 УК РФ (развратные действия, совершенные в отношении лица, заведомо не достигшего 14-летненго возраста). По данным следствия, М. в социальной сети «ВКонтакте» познакомился с 13-летней девочкой, прожи-

[63] См.: Смирнов А.А. Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети Интернет // Система профилактики преступности: современное состояние, проблемы и перспективы развития. СПб., 2013. Ч. 2. С. 40.

[64] См.: Польшиков А.В., Серов Ю.В. Преступления, связанные с изготовлением и оборотом детской порнографии в сети Интернет: проблемы детерминации и предупреждения // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж: Воронежский ин-т МВД России, 2017. № 1. С. 42–50.

вающей в Екатеринбурге. Зная, что переписывается с несовершеннолетней, злоумышленник отправлял ей файлы, содержащие предложения и фотоснимки, «направленные на формирование безнравственного непристойного поведения и содержащие сексуально циничные разговоры»[65].

Существование сайтов, содержащих порнографические материалы с участием несовершеннолетних, определенно способствует увеличению числа сексуальных преступлений в отношении несовершеннолетних. В ходе многолетних исследований, проводимых как в России, так и за рубежом, установлена прямая зависимость роста количества сексуальных преступлений от развития порноиндустрии, в частности, детской и связанной с насилием. Педофилия виртуальная провоцирует развитие педофилии реальной.

Кроме того, психологами доказано, что нет ни одного любителя детской порнографии, который ограничился бы только картинками. Педофилы выходят в социальные сети, чтобы получить откровенное фото детей. Затем начинают шантажировать их, а значит – управлять.

Так, в один из территориальных органов МВД России обратилась гражданка В. с заявлением о том, что ее малолетняя дочь вступила в переписку в Интернете в социальной сети «ВКонтакте» с неизвестным лицом. В ходе общения у ее дочери завязались доверительные отношения с неизвестным, они стали вести разговоры на темы половых отношений и по мере развития такого общения дочь передала несколько фотографий интимного содержания неизвестному. Впоследствии он под угрозой распространения данных фотографий стал требовать от малолетней материалы более извращенного и жесткого характера. Испугавшись, дочь рассказала все матери[66].

Зафиксированы случаи сексуальной эксплуатации собственных детей.

Так, в марте 2017 г. в г. Актау, Казахстан, по результатам проведенной оперативной проверки задержан педофил, который занимался развращением своей малолетней внучки, а также размещением на закрытых сайтах порноматериалов с ее участием[67].

В зарубежных странах для обозначения действий совершеннолетнего лица, направленных на установление в Интернете доверительного контакта с ребенком с целью склонить его к вступлению в

[65] См.: Портал ПРАВО.RU. URL: http: // pravo.ru/news/view/62676 (дата обращения: 29.11.2017).

[66] По данным ГУУР МВД России.

[67] По информации МВД Республики Казахстан.

сексуальную связь, используется термин «кибергруминг», или «онлайн груминг»[68].

Термин «груминг» происходит от английского слова «grooming» – уход, забота. Суть этого метода – создать у ребенка ощущение, что о нем заботятся, им искренне интересуются, вызвать у него ощущение психологической связи, завоевать доверие ребенка или подростка на основе его интересов. Этим понятием охватываются как действия, преследующие цель получения лицом, страдающим расстройством сексуального предпочтения (педофилией) (далее – педофилом), сексуального удовлетворения, так и действия, направленные на вовлечение ребенка в коммерческую сексуальную эксплуатацию.

Типичный механизм груминга заключается в том, что злоумышленник общается в Интернете с ребенком, выдавая себя за ровесника либо ребенка немного старше. Знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить дружеские отношения и перейти на личную переписку. Общаясь лично, он входит в доверие к ребенку, пытается узнать номер мобильного телефона и договориться о встрече[69].

Как показывает анализ оперативной обстановки в Российской Федерации, число преступлений против половой неприкосновенности несовершеннолетних, в том числе совершаемых в сети Интернет, постоянно растет. Так, количество зарегистрированных преступлений против половой неприкосновенности несовершеннолетних в России составило: в 2014 г. – 8490, в 2015 г. – 12 175, в 2016 г. – 12 353. За последние десять лет в России в 25 раз возросло число пользователей сети, а количество домогательств к детям – в 30 раз. В 2016 г. зарегистрировано 455 преступлений по ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», 193 преступления по ст. 242.2 УК РФ «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов».

Однако установить в общем числе вышеуказанных деяний долю преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети Интернет, не представляется возможным, так как статистикой они из общего массива зарегистрированных преступлений не выделяются.

---

[68] См.: Смирнов А.А. Указ соч.

[69] См.: Коммуникационные риски // Линия помощи «Дети онлайн». URL: http: // detionlain.com/helpline/risks (дата обращения: 18.04.2017).

По оценкам специалистов, в сети присутствует не менее 100 тысяч сайтов, в той или иной степени имеющих отношение к детской порнографии.

Нередко продукция такого рода поступает на мировой рынок через российский сегмент Интернета. Все более заметно это направление преступной деятельности переходит под контроль организованной преступности. За последние годы сформировался обширный международный рынок детской порнографии, ставший одним из самых прибыльных секторов теневой экономики. Ежегодно до миллиона детей вовлекаются в участие в этом преступном бизнесе, который приобретает транснациональный характер[70].

Анонимность сетевого общения педофилов существенно облегчает для них обмен идеями, фантазиями, советами, информацией о потенциальных жертвах и способах ухода от ответственности, поскольку раньше педофилам приходилось с большим риском встречаться в специально созданных для этой цели клубах. Интернет же предоставляет им уникальные условия для поиска жертв, позволяя неопределенно долго, анонимно наблюдать за местами сетевого общения детей, изучать подробности их жизни, интересы, особенности характера.

Основные способы совершения преступления педофилами:

в рамках организации производства порнографической продукции – фото- и видеосъемка;

сбор из различных источников и распространение чужих «произведений»;

размещение на своих информационных ресурсах в Интернете ссылок на конкретные сайты, содержащие порнографические изображения несовершеннолетних (рекламирование).

Следует отметить, что чаще всего лица указанной категории занимаются не изготовлением порнографических материалов, а копируют их на других ресурсах или просто выкладывают на своих страничках в социальных сетях ссылки на порнографические материалы («репостят») и ведут обмен с другими Интернет-пользователями.

[70] См.: Осипенко А.Л. Уголовно-правовые и иные средства противодействия обороту материалов с порнографическими изображениями несовершеннолетних в сети Интернет // Уголовное право. 2007. № 1. С. 110.

В соответствии с положениями Европейской Конвенции по борьбе с киберпреступностью, вступившей в законную силу в июле 2004 г.[71], порнографические материалы делятся на три типа:

отражающие сексуальное злоупотребление с реальным ребенком;

порнографические образы, изображающие явно занятого в сексуальном поведении человека, кажущегося несовершеннолетним;

«реалистичные» образы несовершеннолетнего, явно занятого в сексуальном поведении, в изготовлении которого не были задействованы реальные дети.

Отмечается тенденция снижения возраста пользователей сети Интернет, а соответственно – потенциальных жертв. Сейчас это дети в возрасте от шести до девяти лет. Обычно они выкладывают в сеть всю информацию о себе. В соответствии с результатами исследования «Дети России онлайн», российские школьники обычно выходят в Интернет в своих комнатах (70 %), и дома у друзей (50 %), когда возможность контролировать их действия со стороны взрослых минимальна. Причем чем старше школьники, тем реже их контролируют родители: 70 % учеников 9-10 лет и свыше 90 % школьников старше 13 лет пользуются Интернетом бесконтрольно в отсутствие взрослых. Исследование подтвердило и недостаточный уровень владения навыками защиты в ходе онлайн-общения. Среди детей 11–12 лет безопасно пользоваться Интернетом умеют меньше половины. По мере взросления дети и подростки овладевают такими навыками. Среди детей старше 13 лет таких больше половины. Половина российских детей постоянно знакомится в Интернете с новыми людьми: 40 % признались, что встречались с интернет-знакомыми в реальной жизни[72].

К основным факторам киберпреступности, связанной с детской порнографией и посягательствами на половую неприкосновенность несовершеннолетних, помимо гарантированной анонимности злоумышленников, относится особая виктимность детей и подростков в этой сфере, что объясняется:

социально-психологическими особенностями несовершеннолетних (детям и подросткам свойственны доверчивость к информации и людям, отсутствие полноценного критического мышления, ограниченные возможности оказания физического сопротивления педофилу);

---

[71] См.: Конвенция о киберпреступности ETS185; О подписании Конвенции о киберпреступности: распоряжение Президента Рос. Федерации от 15 нояб. 2005 г. № 557-рп // Собр. законодательства Рос. Федерации. 2005. № 47, ст. 4929.

[72] См.: Смирнов А.А. Указ. соч. С. 42.

притягательностью, престижностью среди детей и подростков виртуального общения в Интернете и пополнения круга виртуальных друзей в социальных сетях, являющихся источником опасности;

анонимностью виртуального общения, в котором потенциальной жертве чрезвычайно трудно сразу распознать личность и намерения контрагента;

недостаточным уровнем социального контроля со стороны части родителей за поведением своих детей в интернет-пространстве;

относительной новизной интернет-педофилии, низким уровнем осведомленности детей и их родителей об этой угрозе и способах защиты от нее[73].

По данным МВД Республики Молдова, интернет-технологии востребованы в производстве порнографических материалов с изображениями несовершеннолетних (детской порнографии), в том числе в результате самопроизводства. Также педофилы и иные преступники осуществляют:

онлайновые беседы сексуального характера, grooming и сексуальное домогательство;

вербовку детей с целью сексуальной эксплуатации и производства детской порнографии, а также выезда за границу для сексуальной эксплуатации детей;

сексуальную эксплуатацию детей посредством видеоконференций;

использование компьютерных программ и онлайновых платформ для сексуальной эксплуатации детей.

Несмотря на успешное противодействие преступной деятельности лиц, занимавшихся подстрекательством несовершеннолетних к самоубийствам, **вовлечение подростков в «группы смерти»** в социальных сетях не утратило свою актуальность. Возникновение в Интернете «групп смерти», аналогичных группам «Киты плывут вверх», «Космический кит», «Белый кит», «Китовый журнал», «Море китов», «Океан китов», «Летающий кит», а также организации онлайн игр с хештэгами #Тихий дом, #морекитов, #f57, #d28, #clubsuiside1528, #sedative, #хочу в игру, #разбуди меня в 4.20, несмотря на успешную работу по противодействию деятельности организаторов такого рода сообществ, обладает высоким потенциалом опасности.

Специалисты выделяют следующие формы (способы) принуждения к самоубийству в Интернете:

[73] Указ. соч.

размещение на информационном ресурсе способов и описаний совершения самоубийства, а остальные поступают по его примеру. Такое поведение людей именуется «Эффектом Вертера», который иногда называют «эффектом медиа-домино» (media-contagion effect);

размещение мультимедийных материалов (фото-, видео- и аудиоконтента, простых текстов и креолизованных текстов. Последние соединяют вербальную и невербальную коммуникацию, поскольку не только содержат определенную информацию, но и выступают инструментом скрытого воздействия (демотиваторы, интернет-мемы, комиксы);

онлайн-переписка[74].

Вербовщики в «группы смерти» действуют в социальных сетях: «ВКонтакте», в «Инстраграме», в «Твиттере». После того как ребенок вступает в игру, кураторы переводят детей в мессенджеры: WhatsApp, Viber и другие, позволяющие распространять мгновенные анонимные сообщения. В результате происходит активное влияние на ребенка или подростка с целью заставить его покончить жизнь самоубийством.

Так, Роскомнадзор с января 2017 г. заблокировал в Интернете более 9 тыс. групп, пропагандирующих суицид. Специалисты Роскомнадзора совместно с социальной сетью «ВКонтакте» создали рабочую группу, в результате только в данной сети более 250 таких групп были заблокированы и удалены[75].

В Узбекистане в феврале 2017 г. при проведении профилактических мероприятий в средних учебных заведениях Ташкента милицией выявлено 36 учащихся, принимающих участие в игре «Синий кит».

В Казахстане полицией только за первые два месяца 2017 г. было зарегистрировано 63 случая вовлечения несовершеннолетних в суицидальные игры, при этом 15 подростков, выполняя задания кураторов, нанесли себе телесные повреждения.

В Беларуси в 2017 г. в Витебске предотвращена попытка самоубийства старшеклассницы, которая планировала сброситься с крыши высотного здания. Еще несколько девочек, порезавших себе вены, были выявлены в Гродно и в том же Витебске.

---

[74] См.: Солдатова Г.В. Цифровое детство: новые риски и безопасность. URL: http://psiholog-rmo.ru/wp/wp-content/uploads/2017/02/20170215-cifrovoe_detstvo.pdf (дата обращения: 11.11.2017).

[75] См.: URL: https://ria.ru/society/20170602/1495632157.html (дата обращения: 29.11.2017).

В Молдове только в марте 2017 г. покончили жизнь самоубийством трое подростков. Одну попытку детского суицида полицейским удалось предотвратить. Еще 47 учащихся были уличены полицейскими, проводящими профилактические мероприятия в общественных местах, в выполнении опасных заданий интернет-кураторов.

Количество жертв «синих китов» на территории государств – участников СНГ растет. 29 ноября 2017 г. на 15-м заседании генеральных прокуроров государств – членов Шанхайской организации сотрудничества в Петербурге было объявлено о новой вспышке суицида среди подростков в Кыргызстане. По мнению Генерального прокурора Республики И.Ы. Жолдубаевой, в Кыргызстане становятся популярными суицидальные сообщества в социальных сетях, с начала года зарегистрированы более 20 сообщений. В начале 2017 г. в Кыргызстане получили популярность среди подростков суицидальные игры в социальных сетях, в том числе «Синий кит». По фактам доведения до самоубийств подростков и вовлечения их в эти игры зарегистрированы 22 сообщения. Генеральная прокуратура Кыргызстана подала иски об ограничении доступа к подобным группам и аккаунтам в различных соцсетях, заявления были удовлетворены судами[76].

Криминализация в Российской Федерации в 2017 г. склонения к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ) и организации деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ), с введением в эти нормы квалифицирующего признака в виде способа совершения таких деяний «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)», а также введение уголовной ответственности за вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2 УК РФ) является важным этапом реализации мер уголовной политики в противодействии «группам смерти».

Тем не менее проблема использования высоких технологий для склонения и принуждения несовершеннолетних к самоубийству сохраняет актуальность, поскольку организация соответствующей

[76] «Синий кит» «доплыл» до Киргизии. URL: http://www.rosbalt.ru/piter/2017/11/29/1664696.html (дата обращения: 29.11.2017).

страницы в социальных сетях либо сайта представляется весьма успешным коммерческим проектом: высокий уровень посещаемости позволяет размещать рекламу на выгодных условиях.

В этом отношении видится насущным приведение модельного уголовного законодательства СНГ и уголовных законов стран Содружества в соответствие реалиям современности, требующим защитить подрастающее поколение от опасного контента в Интернете.

Использование информационных технологий с целью совершения преступлений террористического и экстремистского характера

На протяжении многовековой истории терроризма менялись его формы, методы и средства совершения террористических актов, но при этом неизменным оставалась сущность этого явления как насильственного средства экстремистской практики. Эффект террористического устрашения достигается не только за счет террористических акций, совершаемых, как правило, способом, влекущим многочисленные жертвы и разрушения, не только систематическим повторением актов терроризма, но и в значительной мере их публичностью, которая достигается тиражированием информации о террористических акциях с применением телеканалов, радиоэфира, печатных изданий, распространением в сети Интернет экстремистскими и террористическими организациями сведений о своей причастности к совершению конкретных террористических актов и заявлений с угрозами их повторения.

Роль Интернета в расширении пропаганды терроризма в наши дни очень велика. Сама террористическая деятельность, направленная на реализацию экстремистских целей, представляет собой сложное явление, включающее в себя, наряду с планированием и совершением террористических актов, организацию работы по подысканию и вербовке новых членов террористических организаций. Этим, прежде всего, объясняется стремление экстремистских и террористических организаций к проникновению в мировое информационное пространство, поскольку информационные сети и сервисы стали удобным и эффективным средством и одновременно основной информационной площадкой распространения экстремистской идеологии. Наиболее активным пользователем в интернет-пространстве является молодежь в возрасте до 25 лет. Это, на наш взгляд, обусловило эффективность вовлечения молодежи в преступную деятельность

террористических организаций, например в деятельность международной террористической организации «Исламское государство» (ИГИЛ), где массовой вербовке способствовала широкая пропагандистская работа, направленная на создание образа самой мощной террористической группировки, действующей во имя достижения навязанных в массовом сознании ложных идеалов. Ключевую роль в этом сыграла работа сообщества данной организации в социальных сетях и информационных ресурсах Интернета: совмещая привлекательную идеологию, десятилетние традиции производства медиаконтента, приобретя обширную сеть сторонников, боевики смогли достичь высокой популярности. В молодежной среде наблюдается также и феномен «самовербовки» в «ИГИЛ», когда воззрения пользователей резко радикализируются под влиянием распространяемой пропаганды.

Технологии, применяемые в пропагандистско-вербовочной деятельности международных террористических организаций с использованием сети Интернет, требуют выработки конкретных мер противодействия и соответствующей комплексной организации контрпропаганды органами внутренних дел (полиции) государств – участников СНГ.

Электронный терроризм – еще один вид террористической деятельности – может легко осуществляться через Интернет. Эксперты не исключают возможность атак на жизненно важные инфраструктуры через компьютерные сети. В отличие от террориста, кибертеррорист использует современные информационные технологии, специальное программное обеспечение, предназначенное для несанкционированного проникновения в компьютерные системы. Торговые центры, экономические организации – это наиболее возможные мишени будущих атак исламских террористов, вынужденных из-за усилившихся мер безопасности направлять свои удары по менее защищенным целям. Другая возможная стратегия террористов – взлом компьютерных систем обороны или систем, обеспечивающих водоснабжение. Атаки кибертеррористов могут нарушить электроснабжение, вызвать сбои в системе управления воздушным транспортом, сети кредитных карт, системе управления неотложной медицинской помощью[77].

[77] См.: Костихин А.А. Интернет как инструмент террористических и экстремистских организаций в психологической войне // Институт Ближнего Востока. URL: http://www.iimes.ru/?p=4737#more-4737/ (дата обращения: 11.11.2017).

Способы совершения кибертеррористических преступлений с учетом доктринальных позиций можно классифицировать следующим образом:

несанкционированное проникновение в атакуемую сеть или перехват управления сетью при помощи взлома, в том числе путем подбора либо хищения идентификационных данных, позволяющих войти в систему (повысить пользовательские привилегии);

применение эксплоита – программного кода или последовательность команд, находящих и использующих уязвимости в программном обеспечении;

распространение компьютерных вирусов, которые модифицируют и уничтожают информацию или блокируют работу вычислительных систем;

введение в программу вирусов – логических бомб, программ, которые запускаются (срабатывают) при определенных условиях (временных или информационных: пятница, 13-е; 1 апреля) для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных);

использование «троянских коней», выполняющих передачу информации на удаленные компьютеры либо иные вредоносные действия без ведома владельца зараженной системы;

средства нарушения и подавления информационного обмена в сетях. К этой категории следует отнести, по нашему мнению, нарушение функционирования серверов и сайтов путем применения DoS/DDoS-атак.

Например, высказывается мнение о том, что вирус «Flame» следует относить к наиболее мощным средствам компьютерного шпионажа и к категории сложного кибероружия. В качестве примера террористической киберугрозы ядерной структуре государства можно привести многократные кибератаки на ядерные системы Ирана посредством заражения компьютерной системы Иранского центра по обогащению урана вирусом «Stuxnet» в 2010 г. и в 2012 г. вирусом «Stars», а еще через год – вирусом «Flame», причинившими значительный ущерб ядерной безопасности Ирана[78].

Также необходимо обратить внимание на то, что, по мнению экспертов, под прикрытием вирусов типа RANSOMWARE, рассчитанных на вымогательство денег, эпидемия которых отмечена

[78] См., напр.: Бураева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма // Проблемы экономики и юридической практики. 2017. № 2. С. 188–190.

в 2016–2017 гг., могут распространяться вирусы, которые направлены на причинение ущерба. Так, в отличие от вирусов WannaCry, Mischa и Petya (также известным как Petya.A, Petya.D[2], Trojan.Ransom.Petya, PetrWrap[2]), которые предусматривают возможность расшифровки данных зараженного компьютера и восстановление его работоспособности, вирус NotPetya («Не Петя», NotPetya[2], ExPetr) лишь маскируется под вымогателя, в то время как его истинная цель – не денежная выгода, а нанесение массового ущерба[79].

Вирус NotPetya версии 2017 г. (по версии «Лаборатории Касперского» ExPetr, то есть «бывший Петр») похож на семейство Petya, но принадлежит к другой категории – он не предполагает возможности расшифровки информации на жестком диске, а уничтожает ее безвозвратно.

Подытоживая сказанное, необходимо отметить, что использование глобального информационного пространства в организационно-коммуникационных целях террористических организаций тоже представляет собой серьезную угрозу для безопасности стран Содружества.

Кроме того, в условиях поражения террористических группировок в боевых действиях на Ближнем Востоке следует ожидать переход террористических атак в киберпространство: разработку и распространение вирусного программного обеспечения, направленного на причинение ущерба электронно-вычислительной технике и технологическим сетям.

Поиск уязвимостей программного обеспечения в целях продажи третьим лицам и иные компьютерные преступления

Вышеописанные способы совершения кибернападений террористической направленности свойственны и аналогичны способам нападений экономической направленности, а также атакам, совершаемым для демонстрации возможностей организованных преступных групп и хакеров-одиночек в целях поиска заказчиков (работодателей).

[79] См.: Герасюкова М. Петя стирает память // Газета.ru. 2017. 29 июня. URL: https://www.gazeta.ru/tech/2017/06/29/10752467/petya_the_destroyer.shtml (дата обращения: 19.11.2017).

Известны сервисы по поиску определенных уязвимостей в корпоративных сетях с последующей их продажей третьим лицам. Необходимо отметить, что злоумышленники, внедряющие вредоносное программное обеспечение, активно исследуют программное обеспечение и сервисы операционных систем для выявления угроз «нулевого дня» – ошибок в программном обеспечении, приводящих к повышению пользовательских привилегий, о которых неизвестно даже разработчику[80].

Уязвимости «нулевого дня» влекут за собой появление новых способов распространения вредоносного кода, что активно используется киберпреступниками для создания эффективного механизма заражения. Наибольший риск для пользователей создают именно продукты массового использования, такие как популярный «Adobe Reader», «Microsoft Office» и «Adobe Flash Player». Эксплуатация данных уязвимостей осуществляется через так называемые связки эксплойтов, реализующие удаленный доступ к операционной системе с последующей загрузкой вредоносного программного обеспечения.

Значительная часть уязвимостей «нулевого дня» – это критические уязвимости, то есть бреши, позволяющие хакеру получить полный контроль над системой. В течение периода «нулевого дня» злоумышленники имеют наилучшие условия для атак: готовый хакерский эксплойт, а также отсутствие доступных исправлений и антивирусных сигнатур. При этом многие пользователи игнорируют необходимость установки исправлений программного обеспечения даже после их выхода – в особенности для программного обеспечения, не входящего в состав операционной системы.

Недавнее зарубежное исследование показало, что период «нулевого дня» продолжается довольно долго – в среднем 10 месяцев. Для обнаружения уязвимостей вирусописатели используют различные методики, например:

реверс-инжиниринг либо дизассемблирование программного кода и последующий поиск ошибок в алгоритмах работы программного обеспечения;

ruzz-тестирование – «стресс-тест» для программного обеспечения, суть которого заключается в обработке программным обеспече-

[80] Происхождение термина «угроза нулевого дня» связано с тем обстоятельством, что уязвимость или атака становится публично известна до момента выпуска производителем программного обеспечения исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от нее).

нием большого объема информации, содержащей заведомо неверные параметры.

После обнаружения уязвимости в программном обеспечении начинается процесс разработки вредоносного кода, использующего обнаруженную уязвимость для заражения отдельных компьютеров или компьютерных сетей. Помимо создания вредоносных программ, использующих уязвимости нулевого дня в программном обеспечении, вирусописатели активно работают и над созданием вредоносных программ, недетектируемых антивирусными сканерами и мониторами. Данные вредоносные программы также попадают под определение термина «нулевого дня». Как показывает практика, универсальной защиты от угроз «нулевого дня» к настоящему времени не существует[81].

Проведение как точечных атак, так и масштабных заражений в составе бот-сетей возможно посредством «лоадеров» (загрузчиков) вредоносных компьютерных программ, которые, запускаясь на компьютере, загружают в операционную систему сторонние программы, предназначенные как для первичного заражения корпоративных серверов, а также отдельных персональных компьютеров пользователей сети Интернет, так и для их удаленного администрирования (так называемые Remote Administration Too!, RAT).

В заключение необходимо отметить, что исследование выявило отсутствие четкой конкретизации и единого подхода в терминологии, применяемой при осуществлении количественного учета и классификации новых способов совершения преступлений в сфере информационных технологий, что вносит сложность в определениях реальной степени их угроз.

В целях преодоления выявленного несоответствия в работе предложена типология этих преступлений, которая дает возможность создать единый механизм учетно-аналитических операций при оценке состояния и динамики кибепреступности на территории государств – участников СНГ, а также обосновать практические рекомендации и определить пути сотрудничества в этой сфере.

Противодействие использованию информационных сетей преступными группами, специализирующимися на вымогательствах, мошенничествах и кражах, совершении преступлений в сфере компьютерной информации, а также защита важнейших информационных инфраструктур от кибератак имеют ключевое значение для

[81] По информации СОРБ.

внешней и внутренней безопасности как отдельно взятых государств, так и стран Содружества в целом. Решение этой задачи предполагает совместную работу правоохранительных и иных государственных органов, выстраивание взаимодействия и обмена информацией на национальном и межгосударственном уровне, а также выработку и реализацию комплекса нормативно-правовых и организационных мер по противодействию деятельности террористических и иных преступных организаций и сообществ. Необходимо вырабатывать, внедрять и применять совместные меры информационного реагирования и контрпропаганды.

3. СОТРУДНИЧЕСТВО МВД (ПОЛИЦИИ) ГОСУДАРСТВ – УЧАСТНИКОВ СНГ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПУТИ ЕГО СОВЕРШЕНСТВОВАНИЯ

На территории стран Содружества вопросам сотрудничества органов внутренних дел (полиции) по противодействию преступлениям в сфере информационных технологий уделяется большое внимание. За последнее время создана основополагающая нормативно-правовая база, определяющая перспективы его развития и пути совершенствования.

Так, в октябре 2008 г. Решением Совета глав государств СНГ утверждена Концепция сотрудничества государств – участников в сфере обеспечения информационной безопасности. В ходе Минского (октябрь 2013 г.) саммита глав государств СНГ была одобрена Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий. На заседании глав правительств СНГ 20 ноября 2013 г. в Санкт-Петербурге было принято Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности.

Межпарламентской ассамблеей СНГ приняты Рекомендации по совершенствованию и гармонизации законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, которые направлены на установление общих подходов к правовому регулированию обеспечения информационной безопасности, укреплению и обеспечению сбалансированности национальных правовых систем в условиях информатизации общества, на развитие международного информационного обмена, обеспечение безопасности информационных условий экономического и таможенного сотрудничества, на стимулирование использования информационно-коммуникативных технологий в социальной и культурной сфере[82].

Созданная нормативно-правовая база предполагает выработку такой формы организации противодействия преступлениям в сфере

[82] Приняты на тридцать восьмом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ. (О рекомендациях по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере информационной безопасности: постановление Межпарламентской Ассамблеи государств – участников СНГ от 23 нояб. 2012 г. № 38-20).

информационных технологий, которая представляет собой систему комплексных правовых и организационных мер, направленных на профилактику, выявление и пресечение этих преступлений.

Таким образом, совершенствование деятельности органов внутренних дел (полиции) стран Содружества по борьбе с преступлениями в сфере информационных технологий на территории государств – участников СНГ заключается в первую очередь в активизации профилактической работы с потенциальными киберпреступниками и, прежде всего, подростками и молодежью, обладающими навыками программирования, а также специалистами в сфере IT-технологий. Упор в таких кампаниях должен быть сделан на разъяснение последствий противоправной деятельности для тех, кто преступил черту закона. Профилактические и оперативно-профилактические меры должны разрабатываться и осуществляться применительно к различным видам преступлений и сферам преступной деятельности, с учетом типов преступного поведения и способов совершения преступлений.

В связи с этим возможно считать первоочередным:

совершенствование методики выявления и пресечения киберпреступлений;

сбор, обобщение и анализ информации, в том числе оперативной, о конкретных видах преступлений и способах их совершения, об организованных преступных группах, их действиях, связях, финансировании, оснащенности и передвижениях внутри государств – участников СНГ и за их пределами;

обеспечение координации деятельности правоохранительных органов, которые могут и должны участвовать в борьбе с преступлениями в сфере информационных технологий;

организацию технической, правовой, психологической, экономической, финансовой подготовки сотрудников правоохранительных органов, органов внутренних дел (полиции) стран Содружества, участвующих в борьбе с преступлениями в области информационных технологий, поскольку данный вид преступлений очень часто связан с финансовыми и валютными махинациями, преступлениями в сфере экономики;

выработку мер в рамках компетенции органов внутренних дел и соответствующих правил, которые позволяют обеспечить эффективный контроль за цифровой средой, в том числе за передвижением финансов сомнительного происхождения, оборотом средств электронных расчетов, электронных суррогатов денег и иных средств платежей, включая криптовалюты.

Следует признать необходимой адаптацию рекомендованных международными организациями методик по противодействию отмыванию преступных доходов, проникновению криминального капитала в легальную экономику, с одной стороны, и трансграничное его перемещение в целях вывода из юрисдикции стран Содружества, с другой стороны, посредством применения электронных платежных систем, электронных суррогатов денег и ценных бумаг.

Поскольку значительная часть электронных следов компьютерных преступлений носит временный характер, вопрос обеспечения хранения и сохранности электронных данных, относящихся к делу, имеет первостепенное значение. Одной из главных проблем всех правоохранительных органов является отсутствие согласованных на международном уровне условий хранения операторами связи информации. В то время как правительства многих стран возложили на расположенных на их территориях операторов связи обязанность хранения данных в интересах правоохранительных органов, на международном уровне не существует единого общепризнанного стандартного срока, в течение которого каждый оператор связи обязан хранить соответствующую информацию. В результате в тех странах, где на операторов связи возложена подобная обязанность, правоохранительные органы могут быть в какой-то степени уверены в сохранности необходимых данных, что нельзя сказать о тех случаях, когда требуется получение сведений от операторов другой страны.

Традиционные механизмы правовой взаимопомощи и принцип суверенитета, одним из проявлений которого является то, что только правоохранительные органы государства могут производить следственные действия на его территории, требуют множества формальных согласований, делая, по мнению МВД Республики Беларусь, раскрытие и расследование транснациональных киберпреступлений проблематичным, а порой невозможным.

В ходе дискуссий на различных межгосударственных площадках полицейского сотрудничества отмечаются и иные проблемы международного взаимодействия при расследовании компьютерных преступлений. К числу существенных проблем подобного рода можно отнести задержки или отказы в удовлетворении запросов о правовой помощи. В некоторых случаях это было результатом несовместимости уголовной нормативной базы, а в других – следствием ограничений ведомственных нормативных правовых актов.

Практика проведения оперативно-розыскных мероприятий показывает, что фактически все международные кардерские и хакерские группы когда-либо пользовались услугами отдельных разработчиков ВПО, в результате чего эффективно применяли в своей противоправной деятельности сторонние программы для удаленного администрирования персональных компьютеров. Кроме того, известны случаи сервисов по поиску определенных уязвимостей в корпоративных сетях с последующей их продажей третьим лицам.

Информационные технологии позволяют разрабатывать новые изощренные и тщательно замаскированные виды преступного поведения. Возможность сращивания киберпреступности с террористическими организациями представляет собой особую опасность для общества. Поэтому необходимо вырабатывать и применять правовые, экономические, оперативно-розыскные и иные меры по недопущению взаимодействия представителей террористических сообществ и членов преступных группировок, специализирующихся на совершении высокотехнологичных преступлений, или разрыву уже существующих связей такого рода.

Решение таких задач требует совершенствования правовых и организационных основ оперативно-розыскной деятельности и международного сотрудничества по уголовным делам в рамках СНГ путем их приведения в соответствие реалиям развития коммуникационных сетей и экономических отношений.

С позиции применения информационных технологий в разработке новых способов совершения преступлений, представляющих повышенную опасность для интересов государств – участников СНГ, с одной стороны, и профилактической работы – с другой, целесообразно выделить следующие основные направления:

общеуголовные преступления, совершаемые посредством применения цифровых технологий (мошенничества, вымогательства, кражи);

экстремистскую деятельность и терроризм;

незаконный оборот огнестрельного оружия, его основных частей, боеприпасов, взрывчатых веществ или взрывных устройств, включая их хищение и вымогательство;

незаконный оборот наркотических средств, психотропных веществ или их аналогов, растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, прекурсоров наркотических средств или психотропных веществ, а также растений,

содержащих прекурсоры наркотических средств или психотропных веществ, новых потенциально опасных психоактивных веществ;

незаконные изготовление и оборот порнографических материалов или предметов, в том числе материалов или предметов с порнографическими изображениями несовершеннолетних;

преступления экономической направленности;

преступления в сфере компьютерной информации.

Приоритетным направлением работы в рамках информационного противодействия вербовочной деятельности террористических организаций должен стать мониторинг информационной активности членов террористических и экстремистских организаций и ее документирование. Для решения этих задач могут использоваться новые технологии автоматизированного сбора и анализа информации в информационно-телекоммуникационных сетях по технологиям «больших данных» (big data), block chain и data mining.

Сети индустриального Интернета являются привлекательным объектом для террористических атак. Противодействие такого рода угрозам в рамках юрисдикции одного государства, возможностей сил и средств специализированных подразделений его правоохранительных органов представляется затратным и малоэффективным, поскольку указанная преступная деятельность носит преимущественно транснациональный характер.

В связи с этим очевидна необходимость организации сетевого мониторинга террористических техногенных угроз межгосударственного (наднационального) уровня одновременно с унификацией и стандартизацией сетевых протоколов, средств криптозащиты и защиты от несанкционированного проникновения в рамках цифрового пространства СНГ.

Необходимо создать действенную систему обмена информацией о лицах, участвующих в разработке программной продукции и оборудования, используемых для сбыта наркотиков, создателях интернет-сайтов и страниц в социальных сетях, на которых размещается информация о сбыте наркотических средств и психотропных веществ, а также о лицах, осуществляющих рекламу таких ресурсов.

Перечисленные направления совершенствования борьбы с преступлениями в сфере информационных технологий на территории государств – участников СНГ не являются исчерпывающими, однако дают представление о наиболее актуальных криминальных угрозах и путях их нейтрализации.

В связи с изложенным в качестве перспективной задачи видится создание на межгосударственном уровне Центра (подразделения, рабочей группы, действующей на постоянной основе, возможно в составе БКБОП) ситуационного предупреждения киберпреступлений, в компетенцию которого следует включить:

моделирование ситуаций, угрожающих интересам обеспечения безопасности государств – участников СНГ;

выработку мер предупреждения преступлений в сфере информационных технологий, а также методов их выявления и пресечения;

организацию и координацию проведения в рамках Содружества Независимых Государств комплексных совместных и (или) межведомственных профилактических, оперативно-розыскных мероприятий и специальных операций.

На эффективности взаимодействия МВД (Полиции) государств – участников СНГ положительным образом будет сказываться организация комплексного межгосударственного исследования факторов, состояния, динамики и тенденций развития киберпреступности на территориях стран Содружества, которое позволит своевременно определять новые криминальные угрозы и вызовы, вырабатывать соответствующие меры противодействия, а в целом наносить упреждающий удар.

С целью совершенствования правовых основ международного сотрудничества в указанной сфере возможно принять ряд организационных мер по унификации национального законодательства государств – участников СНГ в части противодействия киберпреступности.

В настоящее время отмечаемое несовершенство понятийного аппарата в указанной области существенно затрудняет решение многих нормотворческих и правоприменительных задач. Поэтому в качестве первого этапа в приведении правовой базы международного сотрудничества по противодействию новым способам совершения преступлений видится разработка глоссария, согласованного и одобренного на межгосударственном уровне. Разработка определений, понятий, унификация и акцепция терминологии на межгосударственном уровне станет основой эффективного взаимодействия органов внутренних дел (полиции) стран Содружества в рассматриваемой сфере.

Представляется целесообразным создание рабочей группы по мониторингу законодательства в сфере противодействия киберпреступлениям, к основным функциям которой следует отнести:

выявление и фиксацию, анализ и криминалистическое исследование новых, появляющихся по мере развития цифрового пространства, способов совершения преступлений в сфере информационных технологий;

подготовку предложений по криминализации и последующей квалификации соответствующих деяний;

выработку нормотворческих предложений по унификации законодательства стран Содружества в области противодействия новым преступлениям в сфере информационных технологий;

методическое сопровождение организации межгосударственного сотрудничества в области оказания правовой помощи по уголовным делам по противодействию таким угрозам.

Еще одним немаловажным направлением сотрудничества является формирование единого подхода к организации противодействия и обучения высококвалифицированных специалистов в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, для чего необходимо в рамках СНГ определить базовую образовательную организацию по подготовке, переподготовке и повышению квалификации кадров в указанной области.

Одним из приоритетов в сотрудничестве государств – участников СНГ остается совершенствование единых подходов в борьбе с киберпреступностью с учетом постоянного эволюционирования и появления новых способов совершения преступлений, а также выработка мер по их предупреждению на территории стран Содружества.

На первоначальном этапе важно определить порядок корректировки существующей стратегии, а также порядок мониторинга ее реализации, что станет основой целеполагания для разработки международных программных и нормативных документов.

Нормотворческая работа и организационные усилия в области противодействия известным и новым преступлениям в сфере информационных технологий должны сочетаться с разработкой, внедрением и развитием двух составляющих обеспечения безопасности высокорисковых и системообразующих объектов, информационных сетей и систем обеспечения безопасности: современных информационно-аналитических инструментов и инженерно-технических средств по противодействию информационным ресурсам международных преступных и террористических организаций.

Учитывая динамику роста новых преступных проявлений в сфере информационных технологий[83], Совет министров внутренних дел государств – участников СНГ на очередном заседании, состоявшемся 28 июня 2017 г. в г. Душанбе, конкретизировал, что назрела необходимость создания и реализации системы совместных мер органов внутренних дел (полиции) стран Содружества в рассматриваемой сфере деятельности.

Для решения данного вопроса предлагается разработать механизм согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран Содружества в сфере современных информационных технологий, включающий регламент проведения соответствующих мероприятий.

В содержание предполагаемого механизма целесообразно включить разделы, касающиеся основных терминов, задач и форм согласованных действий, порядка взаимодействия и информационного обмена органов внутренних дел (полиции) государств – участников СНГ при возникновении критической ситуации в информационной сфере, связанной с распространением и развитием новых видов преступлений, представляющих угрозу для безопасности общества и государства.

Необходимо предусмотреть, что порядок взаимодействия, направления, формы, методы и организационные основы механизма согласованных действий должны осуществляться органами внутренних дел (полицией) государств – участников СНГ в пределах полномочий, предоставленных им национальным законодательством по противодействию преступлениям, совершаемым в сфере информационных технологий.

В качестве основных задач в рамках механизма согласованных действий МВД (Полиции) государств – участников СНГ можно определить: проведение комплексного анализа и прогнозирование криминогенной обстановки; основные направления противодействия преступлениям, совершаемым в сфере информационных технологий; мо-

[83] В 2016 г. в мире было зафиксировано 40 млн киберпреступников, которые совершили около 600 млн преступлений. Темпы роста таковы, что их число ежемесячно увеличивается на три-четыре процента (цифры были озвучены во время сессии «Киберпреступность – одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?», которая состоялась на Международном инвестиционном форуме «Сочи-2016»). (Рос. газ. 2016. 1 окт.).

Только в России число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 г. выросло в шесть раз (с 11 тыс. до 66 тыс.).

ниторинг законодательных и ведомственных нормативных правовых актов по проблемам противодействия рассматриваемым преступлениям; межведомственное взаимодействие и международное сотрудничество по вопросам противодействия преступлениям в указанной сфере.

В качестве форм согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемым на территории стран Содружества, следует определить: обмен информацией, непосредственно относящейся к преступлениям в сфере информационных технологий и лицам, их совершившим; обмен оперативной, статистической, научно-методической и иной информацией для пополнения банков данных об указанных преступлениях; обмен научно-методической, технической литературой, нормативными правовыми актами, программными продуктами и решениями, используемыми в предупреждении, выявлении, пресечении, раскрытии и расследовании киберпреступлений в рамках взаимодействия и обмена опытом.

Оказание содействия на основании запросов органов внутренних дел (полиции) стран Содружества по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере информационных технологий может быть возложено на Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ.

В раздел о порядке взаимодействия органов внутренних дел (полиции) государств – участников СНГ при возникновении критической ситуации в информационной сфере, связанной с распространением и развитием новых видов преступлений, представляющих угрозу для безопасности общества и государства, целесообразно включить сбор информации, на основании которой определяется проблема и разработка комплексных мер, осуществляемых по единому замыслу для эффективного противодействия.

Как представляется, предложенный механизм согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран Содружества в сфере современных информационных технологий, в значительной степени повысит эффективность сотрудничества МВД (Полиции) стран Содружества в рассматриваемой области.

ЗАКЛЮЧЕНИЕ

В заключении подведем итоги работы, сформулируем основные выводы и предложения. Анализ национального уголовного законодательства стран Содружества в сфере борьбы с киберпреступлениями показал, что оно характеризуется относительным разнообразием. Вместе с тем в государствах – участниках СНГ законодательство в указанной сфере соответствует заключенной в г. Будапеште 23 ноября 2001 г. Конвенции Совета Европы о преступности в сфере компьютерной информации и закрепляет следующие группы компьютерных преступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием компьютерных данных; правонарушения, связанные с нарушением авторского права и смежных прав; акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

Как показал анализ, развитие информационных технологий и их проникновение во все сферы человеческой жизни ведет к возникновению новых форм преступных посягательств и криминализации новых деяний, а это в свою очередь – к необходимости выработки эффективных мер борьбы с ними.

Выявление, пресечение и раскрытие преступлений в сфере информационных технологий требует от органов внутренних дел (полиции) государств – участников СНГ совершенствования путей сотрудничества по следующим направлениям: принятие мер профилактического характера; развитие правовых и организационных основ межгосударственного сотрудничества; создание на межгосударственном уровне Центра ситуационного предупреждения киберпреступлений; придание одной из образовательных организаций статуса базовой в рамках СНГ по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Учитывая динамику роста новых преступных проявлений в сфере информационных технологий на территории государств – участников СНГ, назрела необходимость разработки механизма согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран Содружества в сфере современных информационных технологий, включающего регламент проведения соответствующих мероприятий.

Как представляется, предложенный в работе проект механизма в значительной степени повысит эффективность сотрудничества МВД (Полиции) стран Содружества в рассматриваемой области.

ОГЛАВЛЕНИЕ

Введение……...…… 3

1. Правовые и организационные аспекты противодействия преступлениям в сфере информационных технологий на территории государств – участников СНГ…..……..…….. 5

2. Характеристика новых способов совершения преступлений с использованием информационных технологий…….. 22

3. Сотрудничество МВД (Полиции) государств – участников СНГ по противодействию преступлениям в сфере информационных технологий и пути его совершенствования…….…. 64

Заключение…….……...……... 73

План ИД ВНИИ, 2018, поз. 28

Игорь Борисович Колчевский
Валентин Михайлович Журавлев
Андрей Геннадьевич Кузнецов
Оксана Владимировна Демковец
Дмитрий Александрович Брехов

НОВЫЕ СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ТЕРРИТОРИИ ГОСУДАРСТВ – УЧАСТНИКОВ СНГ

Аналитический обзор

Редактор *Е. С. Волкова*
Компьютерная верстка *В. В. Пустовит*

Подписано в печать . .2018 Тираж 30 экз.
Формат 60Х84 $^{1}/_{16}$ Печ. л. 5,0 Уч.-изд. л. 4,0 Заказ № 8

Издатель: ФГКУ «ВНИИ МВД России»
121069, Москва, ул. Поварская, д. 25, стр. 1

Группа ОП ФГКУ «ВНИИ МВД России»