Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ТЕОРИЯ И ПРАКТИКА БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Материалы заочной Международной
научно-практической
конференции
(Минск, октябрь 2019 г.)

Минск
Академия МВД
2020

УДК 004:34
ББК 32.81
Т11

Теория и практика борьбы с компьютерной преступностью :
Т11 материалы заоч. Междунар. науч.-практ. конф. (Минск, окт. 2019 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: Д.Н. Лахтиков (отв. ред.) [и др.]. – Минск : Академия МВД, 2020. – 112 с.
ISBN 978-985-576-256-1.

Рассматриваются правовые и методологические проблемы борьбы с компьютерной преступностью, актуальные вопросы использования современных информационных технологий в этом направлении, инновационные подходы при подготовке специалистов в сфере борьбы с компьютерной преступностью.

Издание предназначено для научных сотрудников, преподавателей, аспирантов, адъюнктов, лиц, обучающихся в высших учебных заведениях юридического профиля, практических работников правоохранительных органов.

УДК 004:34
ББК 32.81

Научное издание

ТЕОРИЯ И ПРАКТИКА БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Материалы заочной
Международной научно-практической конференции
(Минск, октябрь 2019 г.)

Технический редактор *А.В. Мозалевская*
Корректор *М.С. Прушак*

Подписано в печать 04.06.2020. Формат 60×84 $^{1}/_{16}$. Бумага офсетная. Ризография.
Усл. печ. л. 6,51. Уч.-изд. л. 6,27.Тираж 40 экз. Заказ 154.

Издатель и полиграфическое исполнение: учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/102 от 02.12.2013.
Пр-т Машерова, 6, 220005, Минск

ISBN 978-985-576-256-1

УДК 343.98

Т.В. Ахраменко, преподаватель кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь
tatyana.ahramenko@mail.ru

ОСОБЕННОСТИ ОСМОТРА И ИЗЪЯТИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Современная следственная и экспертная практика с очевидностью показывают, что значительная часть криминалистически значимой информации содержится в таких источниках доказательств, как документы, существующие не в традиционном (бумажном) виде, а в электронном. Данная тенденция прежде всего обусловлена рядом преимуществ электронных документов:

электронная документация более компактна и позволяет сосредотачивать большое количество информации на малых носителях;

существенно увеличивается скорость передачи документов по каналам электронной связи;

в процессе документооборота использование электронной документации позволяет существенно сократить материальные затраты на подготовку, передачу, проверку и обработку документов.

В то же время новые методы обработки информации, повышая уровень информированности общества и коэффициент полезности его информационных ресурсов, одновременно увеличивают степень уязвимости информации, в том числе и документов, выполненных с помощью средств компьютерной техники, для постороннего воздействия. В том числе и данные обстоятельства детерминируют особенности электронных документов, которые обусловливают определенные отличия в тактике проведения их осмотра и изъятия.

Основная трудность, с которой сталкивается следователь (лицо, производящее дознание) в данном случае, – отсутствие привычных реквизитов, таких как личная подпись, оттиск печати и т. д. Реквизитом электронного документа, подтверждающим его целостность и подлинность, является электронная подпись, поэтому при осмотре электронного документа в первую очередь необходимо проверить подлинность электронной цифровой подписи при помощи открытого ключа. Если идентичность электронной подписи не установлена, то имеет смысл назначить экспертизу электронной цифровой подписи.

Однако при работе с электронными документами необходимо учитывать также и то, что большинство документов, хранящихся в памяти компьютера, не имеют электронной цифровой подписи (в большинстве

случаев электронной цифровой подписью удостоверяют только официальные документы). В подобном случае говорить об идентификации документа очень сложно, так как такие реквизиты компьютерного документа, как время создания, автор документа, количество строк и символов в документе, размер и пр. могут быть попросту изменены как самим автором, так и любым другим лицом, имеющим доступ к этому документу.

При непосредственном осмотре электронного документа следователь (лицо, производящее дознание) должен учитывать тот факт, что данный документ может быть непригоден для непосредственного восприятия (прочтения) человеком (например, файлы с расширением .lnk, .exe, .dat, .ovl и т. п.). Кроме этого, текстовый файл может быть защищен паролем или другими средствами защиты, что, соответственно, также делает невозможным его непосредственное прочтение.

При осмотре электронного документа должна быть выполнена следующая последовательность действий:

фиксация и отражение в протоколе следственного действия наименования файла, его местонахождение (путь к файлу) и формат (определяется по расширению);

определение таких характеристик файла, как количество страниц, абзацев, символов (чтобы не было оснований полагать, что в дальнейшем в количественное содержание файла были внесены изменения), дата создания, последнего редактирования, распечатки, общее время работы с данным документом;

отражение в протоколе следственного действия, какими словами (или символами) начинается и заканчивается осматриваемый электронный документ;

выявление признаков, свидетельствующих о возможном сканировании документа, в частности характерные: форматирование, изменение букв, замена определенных сочетаний букв другими символами;

распечатка и приложение к протоколу следственного действия осматриваемого электронного документа (факт соответствия распечатанного и осматриваемого электронного документа удостоверяется подписями участников следственного действия);

копирование осматриваемого электронного документа на электронный носитель, который не имеет возможности перезаписи (CD-R или DVD-R диск) для возможности его дальнейшего экспертного исследования (этот факт также отражается в протоколе следственного действия). Носитель, на который производилось копирование электронного документа, снабжается пояснительной надписью с названием файла и реквизитами следственного действия, а также подписями участников следственного действия.

При осмотре файла большого объема возможности диска для его копирования ограничены. В этой связи возможно, и это является отличием от подобных процедур осмотра традиционных (бумажных) документов, его архивирование. Такой факт, разумеется, с описанием процедуры архивации и используемой при этом программы также следует отразить в протоколе следственного действия.

Следует отметить, что если осматривается несколько имеющих значение файлов с содержащимися в них электронными документами, то вышеназванные рекомендации необходимо соблюдать при осмотре каждого из них, при этом такие файлы могут быть скопированы на один диск.

УДК 338.2; 343.9

Ю.Н. Бердникова, аспирант Академии управления при Президенте Республики Беларусь
berdnikova-yn@mail.ru

ОЦЕНКА РИСКОВ ПЕРЕХОДА РЕСПУБЛИКИ БЕЛАРУСЬ НА ЭЛЕКТРОННЫЙ УЧЕТ СВЕДЕНИЙ О ТРУДОВОЙ ДЕЯТЕЛЬНОСТИ ГРАЖДАН

Развитие цифровых технологий, инструментов и возможностей их применения оказывает непосредственное влияние на привычные схемы работы и содержание процесса труда, изменяют формы трудовых отношений, структуру занятости, социально-трудовые отношения.

Цифровая трансформация рынка труда предполагает пересмотр исторически сформировавшихся процессов государственного управления социально-трудовой сферой Республики Беларусь, систематизацию и консолидацию потоков информации, расширение данных, накапливаемых на государственном уровне, позволяющих совершенствовать и повысить качество информационного обеспечения принимаемых управленческих решений.

При переходе к цифровой экономике, отсутствие ведения на государственном уровне учета сведений о трудовой деятельности граждан не позволяет спрогнозировать возможное движение либо высвобождение трудовых ресурсов, запланировать своевременную переподготовку (повышение квалификации) работников для их адаптации к высокопроизводительным рабочим местам.

В рамках исследования проведена оценка вариантов (способов) перехода Республики Беларусь на электронный учет сведений о трудовой

деятельности граждан (цель – комплексный показатель) для повышения эффективности информационного обеспечения социально-трудовой сферы. Особенностью решения задачи является многокритериальная оценка показателя качества, учитывались вероятные выгоды, возможности, издержки и риски. Для решения такой задачи с учетом параметрических зависимостей и обратных связей был выбран метод аналитических сетей Т. Саати (МАС).

На основе МАС построена модель (сетевая структура) исследуемого объекта, содержащая четыре подсети, связанные с соответствующими 12 критериями управления, и проведена оценка трех альтернативных вариантов достижения поставленной цели (рис. 1).

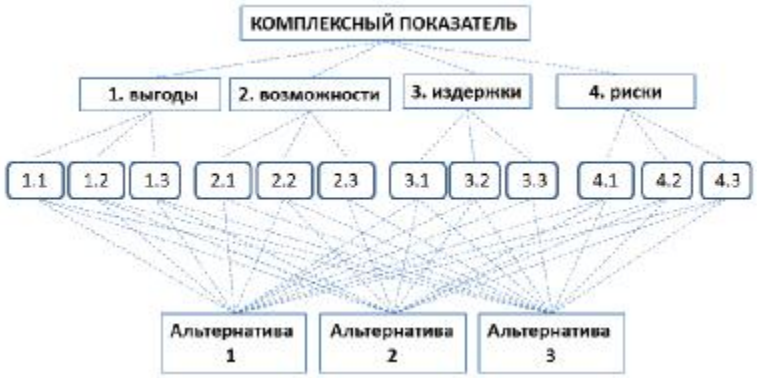


Рис. 1. Сетевая модель

Для расчета комплексного показателя достижения обозначенной цели произведено сравнение следующих трех альтернативных вариантов:

организация учета сведений о трудовой деятельности граждан в рамках расширения функциональных возможностей системы, автоматизирующей ведение индивидуального (персонифицированного) учета (Альтернатива 1);

автоматизация и централизация первичного учета сведений о трудовой деятельности граждан на уровне государства в отдельно создаваемой для этих целей информационной системе (Альтернатива 2);

повышение уровня интеграции данных, характеризующих сведения о трудовой деятельности граждан и содержащихся в государственных, банковских и иных информационных системах (создание информационного ресурса консолидирующего децентрализованные информационные потоки) (Альтернатива 3).

При сравнении указанных выше вариантов достижения обозначенной цели проводилась оценка возможных рисков для каждого из предложенных вариантов. Критерии оценки рисков приведены на рис. 2.

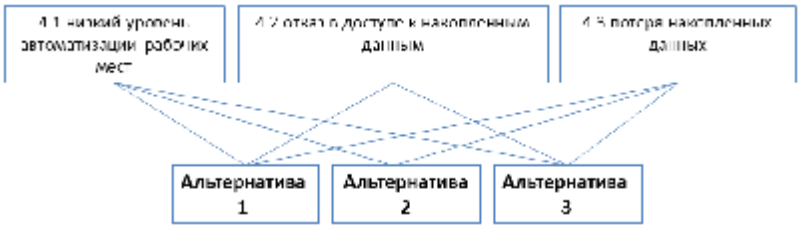


Рис. 2. Критерии подсети «Риски»

На современном этапе развития информационного общества и информационно-коммуникационных технологий нарушение нормального функционирования государственных информационных систем главным образом связано с расширением спектра угроз нарушения дистанционного доступа к данным (в основном для децентрализованных систем), при централизации хранилища данных – с риском потери накопленных данных.

Риск низкого уровня автоматизации рабочих мест в Республике Беларусь в основном связан с тем, что субъектами хозяйствования на персональных компьютерах все еще используется операционная система Windows XP (ОС), которая снята с официальной технической поддержки производителя.

На таких автоматизированных рабочих местах угрозы безопасности в большей мере связаны:

с использованием в указанной ОС устаревшего протокола защиты трафика со слабым алгоритмом шифрования данных, что значительно снижает уровень защиты программного обеспечения, используемого при организации электронного взаимодействия с государственными органами;

ростом угроз со стороны кибермошенников;

риском неправомерных действий со стороны внешних источников в отношении информации, предоставляемой в государственные информационные системы;

возможностью осуществления хакерских атак, результатом которых становятся попытки завладеть информацией.

В процессе принятия оптимального решения проведен анализ указанных выше рисков для каждого альтернативного варианта. Результаты произведенных попарных сравнений критериев в обозначенной

сетевой модели в части критериев, характеризующих риски, представлены в табл. 1.

Таблица 1

Показатель сети	Альтернативы		
	Альтернатива 1	Альтернатива 2	Альтернатива 3
4. Риски			
4.1	0,685422	0,685422	0,090233
4.2	0,234411	0,234411	0,664839
4.3	0,080167	0,080167	0,244928

После построения сетевой модели и проведения оценки парных сравнений, с использованием формул мультипликативной сверки выполнен расчет относительной значимости всех критериев и приоритетов альтернатив, в результате чего определено, что Альтернатива 1 является предпочтительным способом организации на государственном уровне учета сведений о трудовой деятельности граждан на территории Республики Беларусь.

УДК 343.915

В.А. Беспалов, преподаватель кафедры правовой информатики Академии МВД Республики Беларусь
vitalij.bes@inbox.ru

О НЕКОТОРЫХ ТЕНДЕНЦИЯХ РАЗВИТИЯ ПРЕСТУПНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интенсивное развитие во всем мире информационных технологий, сетей передачи данных, сферы телекоммуникационных услуг расширение доступности сети Интернет способствовало появлению киберпреступности. Не обошел данный процесс и Республику Беларусь. В этой связи представляет интерес изучение динамики преступлений, совершаемых в сфере информационной безопасности. Анализ сведений о преступлениях, совершенных в данной сфере несовершеннолетними, привлекает пристальное внимание правоохранительных органов, поскольку для совершения такого рода преступлений обычно достаточно иметь компьютер и выход в сеть Интернет, а современные подростки проводят в интернете большую часть своего времени.

В настоящем исследовании анализируются сведения о зарегистрированных в Республике Беларусь преступлениях, предусмотренных гл. 31

Уголовного кодекса Республики Беларусь (УК) «Преступления против информационной безопасности», с 2010 по 2018 г.

В 2010 г. по ст. 349 УК (Несанкционированный доступ к компьютерной информации) было зарегистрировано 55 преступлений, в 2011 г. – 37 (темп прироста по отношению к предыдущему году составил -32,7 %), в 2012 г. – 30 (-18,9 %), в 2013 г. – 50 (+66,7 %), в 2014 г. – 87 (+74 %), в 2015 г. – 102 (+17,2 %), в 2016 г. – 258 (+152,9 %), в 2017 г. – 462 (+97,4 %) и в 2018 г. – 912 (+118,5 %). Предварительное расследование в 2010 г. окончено по 71 преступлению (следует учитывать, что в число оконченных преступлений могут попадать преступления, зарегистрированные в предыдущих отчетных периодах, но предварительное расследование по которым завершено в текущем отчетном периоде), из них несовершеннолетними совершено 5 преступлений, что составляет 7 %. В 2011 г. предварительное расследование окончено по 40 преступлениям, в 2012 г. – 14, в 2013 г. – 26, в 2014 г. – 50, в 2015 г. – 41, в 2016 г. – 65, в 2017 г. – 138, в 2018 г. – 629, из них несовершеннолетними совершено в 2011 г. 5 преступлений (12,5 %), в 2012 г. – 1 (7,1 %), в 2013 г. – 5 (19,2 %), в 2016 г. – 2 (3,1 %), в 2017 г. – 57 (41,3 %), в 2018 г. – 1 (0,2 %), в 2014 и 2015 гг. преступлений, совершенных несовершеннолетними, не зарегистрировано.

По ст. 350 УК (Модификация компьютерной информации) в 2010 г. зарегистрировано 43 преступления, в 2011 г. – 19 (-55,8 %), в 2012 г. – 17 (-10,5 %), в 2013 г. – 27 (+58,8 %), в 2014 г. – 23 (-14,8 %), в 2015 г. – 37 (+60,9 %), в 2016 г. – 13 (-64,9 %), в 2017 г. – 25 (+92,3 %), в 2018 г. – 9 (-64 %). В 2010 г. предварительное расследование окончено по 35 преступлениям, в 2011 г. – 22, в 2012 г. – 4, в 2013 г. – 29, в 2014 г. – 26, в 2015 г. – 21, в 2016 г. – 15, в 2017 г. – 17, в 2018 г. – 3. Преступления, совершенные несовершеннолетними, зарегистрированы только в 2012, 2013 и 2018 гг. (по одному преступлению, что составило 25 %, 3,4 % и 33,3 % соответственно).

В 2010 г. по ст. 351 УК (Компьютерный саботаж) зарегистрировано 15 преступлений, в 2011 г. – 20 (+33,3 %), в 2012 г. – 24 (+20 %), в 2013 г. – 37 (+54,2 %), в 2014 г. – 83 (+124,3 %), в 2015 г. – 146 (+75,9 %), в 2016 г. – 261 (+78,8 %), в 2017 г. – 207 (-20,7 %), в 2018 г. – 166 (-19,8 %). В 2010 г. предварительное расследование окончено по 6 преступлениям, в 2011 г. – 21, в 2012 г. – 4, в 2013 г. – 12, в 2014 г. – 10, в 2015 г. – 16, в 2016 г. – 61, в 2017 г. – 74 в 2018 г. – 134. Преступления, совершенные несовершеннолетними, зарегистрированы в 2011, 2016, 2017 и 2018 гг. – 1 (4,8 %), 1 (1,6 %), 9 (12,2 %) и 3 (2,2 %) соответственно.

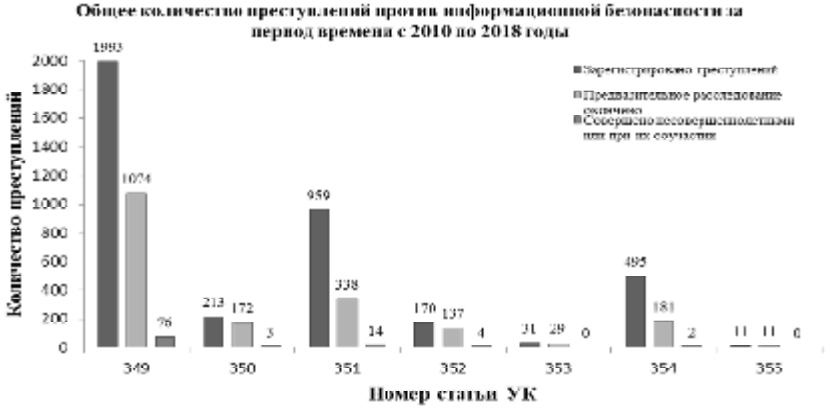
По ст. 352 УК (Неправомерное завладение компьютерной информацией) в 2010 г. зарегистрировано 13 преступлений, в 2011 г. – 3 (-76,9 %), в 2012 г. – 6 (+100 %), в 2013 г. – 42 (+600 %), в 2014 г. – 25 (-40,5 %), в 2015 г. – 13 (-48 %), в 2016 г. – 13 (0 %), в 2017 г. – 29 (+123,1 %), в 2018 г. – 26 (-10,3 %). В 2010 г. предварительное расследование окончено по 11 преступлениям, в 2011 г. – 3, в 2012 г. – 6, в 2013 г. – 13, в 2014 г. – 45, в 2015 г. – 20, в 2016 г. – 11, в 2017 г. – 23, в 2018 г. – 5. Преступления, совершенные несовершеннолетними, зарегистрированы только в 2013 и 2017 гг. – 3 (23,1 %) и 1 (4,3 %) (2,2 %) соответственно.

По ст. 353 УК (Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети) в 2010 и 2011 гг. преступлений не зарегистрировано. В 2012 г. зарегистрировано 3 преступления, в 2013 г. – 5 (+66,7 %), в 2014 г. – 7 (-28,6 %), в 2015 г. – 13 (-48 %), в 2016 г. – 13 (0 %), в 2017 г. – 29 (+123,1 %), в 2018 г. – 26 (-10,3 %). В 2010–2012 гг. преступлений, по которым предварительное расследование окончено, не зарегистрировано, в 2013 г. зарегистрировано 7 преступлений, в 2014 г. – 4, в 2015 г. – 5, в 2016 г. – 6, в 2017 г. – 6, в 2018 г. – 1, при этом преступлений, совершенных несовершеннолетними, в указанный период не зарегистрировано.

По ст. 354 УК (Разработка, использование либо распространение вредоносных программ) в 2010 г. зарегистрировано 12 преступлений, в 2011 г. – 9 (-25 %), в 2012 г. – 29 (+222,2 %), в 2013 г. – 116 (+300 %), в 2014 г. – 32 (-72,4 %), в 2015 г. – 101 (+215,6 %), в 2016 г. – 102 (+1 %), в 2017 г. – 52 (-49 %), в 2018 г. – 42 (-19,2 %). В 2010 г. предварительное расследование окончено по 14 преступлениям, в 2011 г. – 5, в 2012 г. – 4, в 2013 г. – 45, в 2014 г. – 8, в 2015 г. – 4, в 2016 г. – 42, в 2017 г. – 13, в 2018 г. – 36. По одному преступлению, совершенному несовершеннолетними, зарегистрировано в 2012 и 2015 гг., что составило 7,1 % и 25 % соответственно.

По ст. 355 УК (Нарушение правил эксплуатации компьютерной системы или сети) за рассматриваемый период преступления зарегистрированы только в 2011, 2012 и 2013 гг. – 7,3 (-57,3 %) и 1 (-66,7 %) соответственно, таким же является и количество преступлений, предварительное расследование по которым окончено. В исследуемый период преступлений, совершенных несовершеннолетними, не зарегистрировано.

Обобщенно количество преступлений в сфере информационной безопасности за рассматриваемый период представлено на диаграмме.



Приведенные данные позволяют сделать следующие выводы:

для преступности несовершеннолетних в сфере информационной безопасности с 2010 по 2018 г. характерно отсутствие поступательной динамики, в отдельные годы наблюдается резкий рост количества преступлений, совершенных несовершеннолетними, с последующим их падением в другие годы, что, по нашему мнению, вызвано большой латентностью данных преступлений, сложностью обнаружения и фиксации доказательств по данным видам преступлений, а также их многоэпизодностью;

несмотря на незначительное количество преступлений, совершенных несовершеннолетними, в абсолютном выражении их удельный вес в структуре преступлений против информационной безопасности в отдельные годы значительно превышал удельный вес преступлений, совершенных несовершеннолетними, в целом.

Таким образом, невзирая на то, что с точки зрения статистики, преступления, совершенные несовершеннолетними в сфере информационной безопасности, в настоящее время не нашли широкого распространения, развитие криминогенной обстановки в данной сфере в условиях дальнейшего интенсивного развития информационных технологий вызывает определенную тревогу и требует принятия соответствующих средств противодействия преступности несовершеннолетних в сфере информационной безопасности.

УДК 004.8 + 378

Н.М. Бобович, кандидат технических наук, доцент, доцент кафедры правовой информатики Академии МВД Республики Беларусь
n.bobovich@rambler.ru

О КОНЦЕПТУАЛЬНОМ МОДЕЛИРОВАНИИ ТЕЗАУРУСА ТЕРМИНА «КОММУНИКАЦИЯ»

Возрастание интенсивности информационно-коммуникационных процессов, быстрое увеличение объемов информации при одновременном росте числа источников происхождения информации и отсутствии их выраженной взаимосвязи влекут неоднозначность и искажение смысла используемых терминов, что снижает качество коммуникационных процессов.

Актуальное значение данная проблема приобретает в сфере высшего образования, где обучение рассматривается как процесс последовательного расширения и структурирования тезауруса обучающегося посредством усвоения новой информации и приобретения коммуникационной компетентности.

Статья «О концептуальном моделировании тезауруса термина «коммуникация»» посвящена выработке подходов и путей решения важной научно-практической задачи стандартизации термина «коммуникация».

Предлагается методика решения задачи, которая включает три этапа. На первом этапе предлагается разработать словарь тезауруса ключевых терминов, на втором – обосновываются используемые критерии для фильтрации и верификации концептуальной модели тезауруса термина, на третьем – разрабатывается проект концептуальной модели термина «коммуникация». Результаты моделирования представлены в табл. 2.

Таблица 2

Концептуальная модель тезауруса термина «коммуникация»

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина
1		**Историко-этимологический блок** ***Цель*** (назначение) – выяснение истока, происхождения и основных этапов развития
1.1	История коммуникации ***Ист.***	**1,7–2 млн лет назад**. Появление членораздельной речи, слова, языка как ответ на возросшую потреб-

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина
		ность людей в коммуникации. Появление возможности абстрагирования слова от реальности и обмена информацией. Зарождение словесной культуры, религии; разделение труда, переход от присваивающего хозяйства (собирательство, охота на животных) к производящему (земледелие, животноводство, ремесло), создание орудий труда и оружия, развитие обмена, появление транспортных коммуникаций, строительного и военного дела. Появление протогосударств и письменности. **6–3 тыс. лет до н.э.**: появление протогосударств и первых государств; изобретение письменности (Месопотамия, около 6000 г. до н.э.), переход от устной словесной культуры к письменной (*первая коммуникационная революция*). **3 тыс. лет до н.э. – 1 тыс. лет н.э.**: развитие межгосударственных и межцивилизационных коммуникаций, создание империй и межгосударственных союзов, строительство дорог, путей сообщения, переправ и мостов, морских коммуникаций («Все дороги ведут в Рим»); развитие торговли («Великий шелковый путь»); военные походы Александра Македонского; развитие языков и письменной культуры. **1 тыс. лет н.э.**: формирование христианского мира с единой духовной культурой и основными принципами коммуникации (латинский и древнегреческий языки, единое мировоззрение). **IX–XII вв.**: возникновение и расцвет Древней Руси, возникновение и развитие древнерусского языка («Язык до Киева доведет»), водный военно-торговый путь «Путь из варяг в греки». **XIII–XV вв.**: распад Древней Руси, выделение русского, белорусского и украинского языков; образование Великого Княжества Литовского (ВКЛ); развитие печатного дела на основе изобретения Гуттенберга (Германия, 1450) – *вторая коммуникационная революция.* **XVI–XVIII вв.**: ***Франциск Скорина*** начинает белорусское книгопечатание, издает в Праге книгу «Псалтырь» (1517); ученый-гуманист ***Бернард Воевудко*** создает первую типографию в Брест-Литовске (1553); ученый-гуманист ***Симон Будный*** на белорусском языке выпускает в свет книгу «Катехизис» (1562); ***Симеон Полоцкий***, белорусский просветитель, духовный писатель, богослов, организует в Полоцке Братскую школу (1658), пишет книгу «Слово о пользе путешествий» (1666), разрабатывает проект «Славяно-Греко-Латинской Академии» в Москве (1678).

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина
		Конец XIX– середина XX вв.: вхождение слова «коммуникация» в научную терминологию, становление белорусского литературного языка издание первого словаря «Беларуская навуковая тэрміналогія. Менск : Выдавецтва Інстытуту Беларускае Культуры», 1922. **1939–1945 гг. – Вторая мировая война. Победа Советского Союза в Великой Отечественной войне (1941–1945 гг.)**: как определяющий фактор развития мирового сообщества и глобализационных процессов в XX в., а также условие отказа от мировых войн как способа решения глобальных противоречий. Появление глобальных наднациональных институтов, обеспечивающих межгосударственную коммуникацию (ООН и др.). **Конец XX – начало XXI вв.**: создание и внедрение информационно-коммуникационных технологий (ПЭВМ и суперкомпьютер, разработка языков программирования высокого уровня сети Интернет электронные масс-медиа). Цифровая коммуникация *(третья коммуникационная революция*). **2017–2019 гг.**: в России издан словарь «Война и мир в терминах и определениях» в 2-х книгах под общ. ред. проф. Д.О. Рогозина, в котором представлены военно-политическая, военно-техническая и военно-научная терминологии, сделан системный взгляд на современные проблемы войны и мира (включая военные коммуникации). *Примечание*. Персональный вклад белорусских ученых в развитие коммуникации отражается в подразделе «Персоналии».
	Этимология ***Этим.*** […].	**Коммуникация** в русском языке заимствована в Петровскую эпоху из польского языка, где *komunikacja* означала «сообщение» от лат. communicatio, производного от communico «сообщаю» и communis «общий». *Источник*: Этимологический словарь М. Фасмера; [< лат. *communicativus* – «относящийся к передаче, сообщению», < *communicare* – «делать общим; связывать, соединять»]. *Источник*: Современный словарь иностранных слов.
2		**Морфологический блок** ***Цель*** – выявление значения корня термина
2.1	Морфология ***Морф.*** (…)	**Коммуникация** – (корень слова – *коммуник* + суффикс *-ации* + окончание *-я*; основа слова-*коммуникаци)*. Суфф. *-ации* означает «процессуальность или результат действия». Коммуникация – «общий результат действия».
2.2	Родственные слова	Коммуникология, коммуникавистика, коммуника-

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина
		тивность, коммуникативный, коммуникационный, коммуникабельность, коммуникант, коммуникавист, телекоммуникация, телекоммуникационный, информационно-коммуникационный и др.
3	https://ru.wiktionary.org/wiki/%D0%B3%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C-.D0.A1.D0.B5.D0.BC.D0.B0.D0.BD.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B8.D0.B5_.D1.81.D0.B2.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0	**Семантический блок** ***Цель*** – установление семантических связей структуры термина
3.1	Смысл (значение)	Способ связи объектов, перемещение, снабжение, обмен, путь сообщения, общение, сообщение, связь (отношение, знакомство, контакт) и др.
3.2	Синонимы	Связь, сообщение, контакт, общение, биокоммуникация, интеракция, путь сообщения, линия связи, электрокоммуникация (словарь синонимов).
3.3	Антонимы	Атомизация, изоляция, некоммуникабельность, теракция и др.
3.4	Гиперонимы	Интернет-коммуникация, глобальная коммуникация.
3.5	Гипонимы	Электросвязь, энергоснабжение, теплоснабжение, газоснабжение, водоснабжение и др.
3.6	Устойчивые словосочетания	Глобальная коммуникация, мобильная коммуникация, коммуникативное взаимодействие, научные коммуникации, теория коммуникации, интернет-коммуникация, массовая коммуникация, коммуникационные процессы, коммуникационные системы, законы коммуникации, категории коммуникации, инновационные коммуникации, информационно-коммуникационные технологии, коммуникационное сопровождение инновационной деятельности и др.
4		**Классификатор** ***Цель*** – установление полноты определения термина, классификация определений по основным признакам
4.1	Исторические эпохи	Вербальная (словесная) коммуникация; письменность; книгопечатание; электронная коммуникация; цифровая коммуникация и т. п.
4.2	Виды внешней среды	Коммуникация: водная, воздушная, наземная (железнодорожная, автомобильная), подземная (метро, канализация, туннель) и т. п.

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина			
4.3	Сферы деятельности	Коммуникация: информационная, инновационная, образовательная, научная, лингвистическая, инженерная, транспортная, экономическая, социальная, управленческая, культурная, военная и др.			
4.4	Социальное взаимодействие	Коммуникации: организационные (внешние, внутренние; горизонтальные, вертикальные); межличностные (формальные, неформальные) и др.			
5		**Статистический блок** ***Цель*** – вывод общего определения термина. Используется метод контент-анализа			
	Частотный спектр смысла, %	Всеобщая связь Средства связи (универ. смысл)	Пути сообщений Передача, обмен (техн. смысл)	Общение Взаимодействие (соц. смысл)	Способы и средства связи в живой природе
		24	76	–	–
5.1	Нормативные определения	Коммуникация: взаимоотношения между двумя или более лицами, связанными обменом информацией (сообщения, идеи, знания, стратегии и т. д. (МСКО: 2011)); обмен *информацией*, передача *информации* (ИСО 9000-2015); общая функция управления в системе менеджмента качества (ИСО 9001-2015).			
5.2	Определения в словарях	12	66	20	2
		Камунікацыя – абмен думкамі, перадача інфармацыі пры дапамозе мовы (А.М. Булыка, 1993); Коммуникация – общение, взаимодействие в процессе деятельности (Л.А. Кандыбович, 2010).			
5.3	Научные, учебные определения	7	45	44	4
		Коммуникация – обмен информацией, знаниями, интеллектуальной собственностью (Т.М. Орлова, 2012). Коммуникация – способ взаимодействия, опосредованный некоторым объектом (Я.С. Яскевич, 2018).			
6		**Проектирование обновленного определения термина** ***Цель*** – обогащение термина новым смыслом			
6.1	Обобщенное определение	Коммуникация – взаимосвязь и/или связующий процесс, объединяющий множество элементов в единое целое (систему).			
6.2	Альтернативы	Коммуникация – связующий процесс и/или функция управления потоками информации, энергии, материалов и иных ценностей. Коммуникация – процесс передачи информации, энергии или массы (инфо-, энерго-, массопередачи) в условиях неоднородной среды.			

Код	Блоки и их параметры	Русско-английское название термина: коммуникация/communication Основные свойства и характеристики термина
6.3	Экспертиза	Осуществляется экспертами.
6.4	Легитимация	Осуществляется одновременно с утверждением нормативного акта.
7		**Перевод определения термина на иные естественные языки**
7.1	Перевод на белорусский язык	Камунікацыя – узаемасувязь і/або функцыя кіравання патокамі інфармацыі, энергіі, матэрыялаў і іншых каштоўнасцяў.
7.2	Перевод на английский язык	Communication – interrelation and/or function of management of a potokma of information, energy, materil and other values.
Персоналии: (белорусские ученые): Т.Н. Суша (1972), А.М. Широков (1984, 1999), Г.А. Цыхун (1987, 2013, 2018), А.М. Булыка (1993), Н.И. Кабушкин (1996, 2013), А.И. Зеленков (1998, 2016), О.В. Терещенко (2004), Е.М. Бабосов (2004, 2015), Г.Е. Адамович (2006), В.Ф. Берков (2007), А.А. Трусь (2007), Я.С. Яскевич (2007, 2012), Е.Н. Горегляд (2008, 2015, 2017), М.Н. Мазаник (2008, 2016), А.В. Рубанов (2008), И.В. Сидорская (2008, 2012), Л.А. Кандыбович (2010), В.В. Фурс (2011), С.И. Лебединский (2011, 2018), Т.В. Карнажицкая (2012), А.Я. Сарна (2013), Т.Н. Беляцкая (2014), А.А. Широканова (2014), А.В. Кириллова (2014), И.И. Калачева (2016), М.Г. Волнистая (2018) и др.		

С помощью предлагаемой разработанной и апробированной концептуальной модели тезауруса термина «коммуникация» имеется возможность повысить эффективность использования в понимании, освоении, передаче информации и знаний, а также накопить, обогатить и распространить передовой опыт (компетенции), совершенствовать организацию работ в области научной и образовательной терминологии, сфере инновационной деятельности.

УДК 343.985

П.Л. Боровик, кандидат юридических наук, доцент, доцент кафедры правовой информатики Академии МВД Республики Беларусь
P.Borovik@tut.by

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Анализ уголовной статистики свидетельствует, что начиная с конца XX в. по настоящее время на территории стран постсоветского пространства наблюдается устойчивый рост преступлений, совершаемых с

помощью информационных технологий. Речь идет об уголовно наказуемых деяниях не только против информационной безопасности, но и в сфере незаконного оборота наркотических средств и психотропов, изготовления и распространения детской порнографии, противоправных действий экстремистской и террористической направленности, а также иных правонарушениях, совершаемых с помощью различных электронных носителей (компьютеры, ноутбуки, смартфоны и т. д.) и информационно-коммуникационных сетей.

Специфика указанных преступлений и их постоянный рост закономерно предопределяют повышенное внимание широкого круга ученых. В последние годы на страницах юридической печати все больше внимания уделяется вопросам научно-методического обеспечения противодействия таким преступлениям, включая их предупреждение и выявление, а также расследование.

Так, актуальные проблемы противодействия рассматриваемым уголовно наказуемым деяниям своевременно затронуты в научных публикациях В.Б. Вехова, П.В. Миненко, Д.Г. Осипенко, В.В. Полякова, А.Н. Тукало, М.В. Кондратьева, В.Е. Козлова, А.М. Ишина, Е.П. Ищенко, Д.Л. Харевича и других ученых. Несмотря на высокую теоретическую и практическую значимость этих исследований, следует отметить, что они не исчерпывают всех аспектов противодействия преступлениям, совершаемым с использованием информационных технологий. Отсутствие комплексного характера в исследовательской работе в этом направлении ощутимо затрудняет противодействие преступлениям, совершаемым с использованием постоянно совершенствующихся компьютерных и сетевых технологий. В частности, в настоящее время недостаточно проработаны вопросы организации и тактики проведения оперативно-розыскных мероприятий в сети Интернет. В серьезном исследовании нуждаются возможности оперативного поиска и идентификации пользователей в «закрытом» сетевом информационном пространстве, именуемом «DarkNet» (в том числе в неиндексируемом сегменте открытого интернета «DeepNet»). Не в полной мере исследованы и проблемы документирования противоправной деятельности участников преступной деятельности, а также легализации данных, полученных в ходе проведения указанных мероприятий с целью их дальнейшего использования в уголовном процессе. Имеющиеся пробелы не лучшим образом сказываются на практической деятельности сотрудников правоохранительных органов и, несомненно, препятствуют процессу воплощения права, социальной справедливости и осуществлению правосудия в сфере противодействия рассматриваемым преступлениям.

Вышеприведенные обстоятельства обосновывают актуальность осуществления научных изысканий в обозначенной сфере и предопре-

деляют их задачи, связанные с выработкой соответствующих научно обоснованных практических рекомендаций. При этом очевидно, что практическое использование подобных методических материалов требует обязательного наличия основательной профессиональной подготовки, а также регулярного обновления имеющихся знаний у оперативных работников, следователей и, разумеется, специалистов и экспертов.

В контексте затронутой проблемы важно также отметить, что связанное с развитием информационных технологий структурное видоизменение традиционных форм совершения рассматриваемых преступлений, их трансформация в качественно иные не только порождают необходимость изменения организации и тактики противодействия преступности, но и требует новых подходов к системному и институциональному теоретическому осмыслению соответствующих криминологических проблем. Так, на фоне происходящих социальных преобразований особая роль должна отводиться криминологическим научным изысканиям, позволяющим сформировать принципиально новую парадигму противодействия преступлениям, совершаемым с помощью информационных технологий.

Среди перспективных научных направлений, которые ждут своих исследователей, следует отметить и методику раскрытия и расследования преступлений в сфере банковских платежных карточек, а также высокотехнологических мошенничеств. Интересную и вместе с тем сложную тему представляет криминалистическое исследование цифровой информации, технологии работы с электронными следами и большими данными (Big Data), идентификация и диагностика программно-технических средств совершения преступлений. Не нашла своего отражения в рамках отдельной диссертационной либо монографической работы и проблематика соответствующих судебных экспертиз.

В последние годы свидетельства преступной деятельности, представляющие интерес для органов внутренних дел, все чаще обнаруживаются в компьютерных системах, где они содержатся в различных информационных объектах (электронные документы, сообщения электронной почты, вредоносные программы, «облачные» ресурсы и т. п.). Исследование показывает, что основная специфика пространственно-временной локализации подобных объектов неминуемо сказывается на изменении содержания, методов и форм их вовлечения в уголовный процесс. Вместе с тем анализ судебной практики привлекает внимание к спектру проблем, связанных с недостаточной готовностью оперативных и следственных органов к использованию данных, хранящихся в

компьютерных системах. Даже для сетевых компьютерных преступлений в качестве доказательств в подавляющем большинстве случаев используются «традиционные» объекты, в то время как процессуальное значение «электронных документов», как правило, становится ничтожным в результате неумелых действий по их использованию. Очевидно, что в современных условиях электронно-цифровые следы способны существенно расширить доказательственную базу по многим уголовным делам, а потому их эффективному вовлечению в уголовный процесс следует уделять особое внимание, и соответствующие исследования, разумеется, должны быть продолжены.

Таким образом, результаты проведенного анализа свидетельствуют о том, что организация научных исследований по данной тематике требует дальнейшего совершенствования. Среди основных перспективных направлений работы в этой области можно выделить следующие:

организация и тактика проведения оперативно-розыскных мероприятий в сети Интернет;

оперативный поиск и идентификация пользователей в «закрытом» сетевом и неиндексируемом информационном пространстве интернета;

документирование противоправной деятельности участников преступной деятельности, а также легализация данных, полученных в ходе проведения указанных мероприятий с целью их дальнейшего использования в уголовном процессе;

криминологическое исследование проблем совершения преступлений, совершаемых с использованием информационных технологий;

методика раскрытия и расследования преступлений в сфере банковских платежных карточек, а также высокотехнологических мошенничеств;

криминалистическое исследование цифровой информации, технологии работы с электронными следами и большими данными (Big Data) в деятельности по расследованию преступлений;

идентификация и диагностика программно-технических средств совершения высокотехнологических преступлений;

проведение судебных экспертиз по материалам и делам, связанным с совершением высокотехнологических преступлений.

Обозначенные направления научных исследований открывают новые возможности для дальнейшего развития юридической науки и ее практического применения с учетом реалий в настоящее время. В этой связи актуальным является проведение постоянных целенаправленных конференций, круглых столов и других научных мероприятий, посвященных указанным вопросам.

УДК 343.91:004.738.5

О.Н. Брисковская, кандидат юридических наук, ведущий научный сотрудник Национальной академии внутренних дел (г. Киев, Украина)
oksanuhka@ukr.net

ЛИЧНОСТЬ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Ежегодно киберпреступность наносит государствам и частным лицам очень большой вред. Самый распространенный вид преступления – мошенничество в сети Интернет. Чаще всего мошенники создают сайты и продают несуществующий товар, очень много преступлений, касающихся выманивания информации с банковских платежных карточек и онлайн-кредитования. Преступников привлекает скорость, удобство, анонимность интернета и отсутствие границ.

Несмотря на имеющиеся в научной литературе наработки о личности преступников, их недостаточно для формирования целостного, завершенного и полного представления о личности интернет-мошенника, и возможности учета его поведенческих проявлений в процессе расследования таких преступлений. Выделение типовых моделей разных категорий преступников, знание основных черт этих людей позволяет оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск преступника и точнее определить способы установления и изобличения конкретного правонарушителя. Криминалистическая характеристика киберпреступлений отличается от уже известных криминалистической науке преступных посягательств определенной спецификой. В первую очередь в нее должны входить криминалистически значимые сведения о личности правонарушителя, мотивации его преступного поведения, типичные способы, предметы и места посягательств. Мошенники являются хорошими психологами и знают, на какие слабые стороны человеческой натуры можно нажать, чтобы убедить жертву добровольно расстаться с деньгами (малообразованность, жадность, вера в «счастливый случай», жажда «халявы», лень, азарт, тщеславие, несамостоятельность, предрассудки, привычка быть вежливым и соблюдать общественные нормы, ритуалы и традиции, комплексы, невротические состояния и т. д.). Перечислим самые популярные способы на сегодня, которыми интернет-мошенники обманывают людей на покупках в сети Интернет:

схема первая – звонок из банка. Мошенники под видом покупателя звонят продавцу, некоторое время торгуются, потом берут номер банковской платежной карточки, обещая перевести средства, и несколько дней не звонят. Затем звонит «представитель банка» и сообщает, что карточка продавца, якобы была заблокирована для поступления средств от юридических лиц. Чтобы разморозить счет, мошенники предлагают воспользоваться мобильным приложением и выведывают все данные с банковской платежной карточки жертвы;

схема вторая – мошеннический сайт. Более изобретательные мошенники открывают собственные интернет-магазины. Расходы мизерные – сделать сайт можно за несколько тысяч гривен, зато нажиться на нем можно чуть ли не на миллионы гривен. Если лицо заинтересовал определенный товар, его цена, стоимость которого значительно ниже, чем реализуется в других магазинах, то, конечно, лицо интересуется этим товаром, звонит мошенник, он, как правило, просит осуществить предварительно оплату 10, 20, 50 % за несуществующий товар. Или интернет-мошенники делают копию сайта банка, клиент вводит логин (номер телефона) и пароль, как следствие, их получает злоумышленник. Далее приходит sms, что доступ якобы заблокирован, звонит «сотрудник банка» и просит продиктовать код из сообщения. Логин-пароль вор уже знает и код с sms – последнее сведение, чтобы войти в настоящий аккаунт;

схема третья – деньги начислены. Например, вы продаете планшет, игровую приставку или иной товар. Мошенник договаривается с вами о встрече, вдруг сообщает, что не может на нее прийти и предлагает отдать товар его товарищу или курьеру, но после того, как на счет поступят деньги. Вам приходит sms с сообщением о начислении средств, но не от банка, а от обычного частного номера. В большинстве случаев курьером оказывается водитель маршрутки или таксист. Он спешит ехать, и вы, торопясь, отдаете товар уезжающему курьеру.

Интернет-мошенники имеют устойчивую подсознательную антисоциальную направленность. Как правило, в эту категорию входят лица, которые неоднократно совершали такие преступления. По содержанию ценностно-ориентационной направленности это преступники с корыстной направленностью, посягающие на основное достояние общества, – распределение материальных благ в соответствии с мерой и качеством затраченного труда. Мотивация интернет-мошенников – желание «легких денег», стремление к наживе. По статистическим данным, которые приводит Піцик Ю.М. в статье «Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі» в *Науковий вісник Міжнародного гуманітарного університету. Серія:*

Юриспруденція, 2017. № 26. С. 106 (105–107), большинство преступлений в интернете против собственности (79 %) – мошенничества, как правило, совершаются мужчинами (94 %), и лишь в редких случаях женщинами (6 %). Как установлено, такие преступления совершаются лицами, официально не состоящими в браке и не имеющими детей. Количество холостых лиц из общего числа составляет 70 %, в то время как в браке – 30 %. Как показывает судебная практика, 51 % лиц, совершивших преступления в сети Интернет, не имеют постоянного места работы. Среди остальных 49 % большую часть занимают менеджеры низшего и среднего звена, реже встречаются должностные лица и программисты. Так, если средний возраст мошенника в материальном мире составляет от 26 до 39 лет, то средний возраст интернет-мошенника варьируется от 18 до 35 лет. Вообще возраст интернет-мошенников может варьироваться от 18 до 45 лет, а социальное положение в обществе – от студента до сотрудника государственного учреждения или фирмы. Личностный портрет интернет-мошенника характеризуется авантюрным складом, «игровым» типом личности, в большинстве случаев постоянный риск является физиологически необходимым для мошенника, следовательно, такие лица склонны к риску, им присуща решимость, снижена тревожность, обладают самоконтролем и терпением, при этом быстро реагируют на быстро меняющуюся обстановку и легко приспособляются к ней. Как правило, они испытывают интеллектуальное превосходство над жертвой, уверены в себе, имеют нестандартность мышления и поведения, креативность, шарм, обаяние, настойчивость, умеют работать с информацией и быстро реагировать на изменяющуюся информацию.

С развитием интернет-технологий меняются и развиваются новые виды мошенничеств в сети Интернет. Они становятся еще более опасными, так как посягают на частную, конфиденциальную информацию пользователей. С целью получения наживы интернет-мошенники используют преступные приемы, что приводит к негативным последствиям, так как их жертвами становятся не только рядовые граждане, но и частные, и государственные организации. Определение личностных свойств преступников, совершающих мошенничество в сети Интернет, позволит оптимизировать процесс выявления круга лиц, среди которых целесообразно вести поиск мошенника, определять тактику ведения допроса, своевременно выявлять и расследовать такие преступления.

УДК 343.985.7:343.343.3

Н.С. Бушкевич, следователь по особо важным делам управления анализа практики и методического обеспечения предварительного расследования центрального аппарата Следственного комитета Республики Беларусь
n.bushkevich@sledcom.by

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО КАК МЕСТО АККУМУЛИРОВАНИЯ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ О ХУЛИГАНСТВЕ

Придерживаясь традиционно-диалектического подхода в изучении причин эволюции преступности, прогнозировании тенденций и перспектив развития криминальных схем и механизмов, необходимо отметить, что одной из существенных детерминант этих процессов является внедрение в жизнедеятельность общества информационно-коммуникационных технологий.

Сегодня тренд белорусского общества – постепенный переход от традиционного индустриального общества к информационному, причем процессы цифровизации и автоматизации происходят не только на уровне отдельных индивидуумов или сообществ, когда все более совершенные девайсы, гаджеты и софты модифицируют коммуникацию между членами общества, расширяя возможности использования виртуального пространства для этих целей, но и на уровне государственно-частного партнерства. Примером является разработка ряда IT-проектов в рамках реализации стратегии государственной политики «Наука и технологии: 2018–2040», утвержденной на II Съезде ученых Беларуси в декабре 2017 г., которая предполагает переход к цифровой экономике и внедрение информационных технологий во все сферы жизнедеятельности белорусского общества.

При этом если законопослушной частью общества большинство инноваций воспринимаются с настороженностью, скептицизмом и недоверием, а процесс принятия и адаптации характеризуется продолжительностью и сложностью протекания, то преступная часть белорусского общества быстро адаптирует новые IT-возможности, вкрапляя их в механизмы достижения преступного результата, и за счет этого стремительно развивается.

Наиболее проблемным с точки зрения организации правоохранительной деятельности, направленной на защиту интересов общества и государства от противоправных посягательств, является частичный переход преступного мира в виртуальное пространство и использова-

ние его просторов в криминальных целях, при этом речь идет не только о хищении с использованием компьютерной техники или деяниях против информационной безопасности, как это традиционно принято понимать. В настоящее время можно говорить об использовании виртуального пространства, в том числе в качестве средства или элемента механизма совершения многих преступлений общеуголовной направленности. Не является исключением и хулиганство. Как правильно отметил А.Ж. Саркисян, использование интернета и средств IT-технологий в той или иной форме сегодня характерно для совершения преступлений в любой из сфер общественного порядка.

Действительно, умышленные действия, грубо нарушающие общественный порядок и выражающие явное неуважение к обществу (уголовно наказуемое хулиганство), с точки зрения преследуемых целей характеризуются своей открытостью, особенно в случаях совершения в группе. Для лиц, совершающих такие деяния, принципиально важным является не только наступление общественно опасных последствий их хулиганской активности, но и визуализация (или ее возможность) членами общества самого исполнения объективной стороны преступления. В этом аспекте современные информационно-коммуникационные технологии как нельзя лучше позволяют хулиганам демонстрировать свою браваду, дерзость и неуважение к общепринятым нормам поведения и морали отдельным гражданам в различных формах проявления и распространять (транслировать) информацию о своих хулиганских действиях неопределенному кругу лиц с помощью мессенджеров, социальных сетей и интернета. В таких условиях правомерно говорить о виртуальном пространстве как о месте сохранения следов совершенного хулиганства, которые наряду с традиционными для этого преступления материальными и идеальными следами составляют следовую картину.

Рассматривая виртуальное пространство как место создания и аккумулирования электронно-цифровой информации (ЭЦИ) о преступных событиях, происходивших в материальном мире, на наш взгляд, необходимо отметить наличие у ученых многих областей знаний научного интереса к этой категории, в том числе и криминалистики. С точки зрения правового регулирования деятельности человека в виртуальном пространстве наиболее удачное, как представляется, определение данной научной категории дано Н.Н. Телешиной. В ее понимании это область технических, технологических и социальных отношений, возникающих, изменяющихся и прекращающихся в процессе использования компьютерной или иной электронной технической сети по поводу информации, информационных ресурсов, информационных услуг и средств связи. По сути, виртуальное пространство (киберпространство) определенным образом объединяет человеческую и технологическую среду, расширяя возможности людей независимо от национальности, культуры и языка

по созданию, передаче и получению информации через всемирную сеть компьютеров, девайсов, устройств хранения ЭЦИ, взаимосвязанных средствами коммуникационных инфраструктур, обеспечивающих цифровую обработку, хранение и передачу информации.

Для криминалистики виртуальное пространство представляет научный интерес с точки зрения теории отражения. В этом контексте его целесообразно рассматривать как часть информационного пространства, аккумулирующую в себе сведения о лицах, событиях, предметах, явлениях и процессах, имевших место в материальном мире и представленных в математическом (бинарном) виде в процессе движения по компьютерным сетям либо хранящихся в памяти компьютеров, девайсов (т. е. физических электронных устройств) или другого носителя ЭЦИ. Любое действие человека в виртуальном пространстве, будь оно связано с внесением в него новой информации (например, текстовой, звуковой, графической, фотография или видеоинформация) либо совершением с ней действий, включая просмотр, изменение или удаление в компьютерной системе или носителе ЭЦИ, оставляет следы такого воздействия.

Если для киберпреступлений, которые, как правило, совершаются непосредственно в виртуальном пространстве, характерны виртуальные следы в виде log-файлов, поврежденных файловых систем ПК, следов создания (пересылки), запуска вредоносного ПО, вирусов и т. д., то совокупность ЭЦИ, сохранившей в себе сведения об имевшем место в материальном мире акте хулиганства, иная. Встречающиеся на практике способы использования IT-технологий при совершении хулиганства и распространении сведений о нем, а также цели такого применения имеют различное фактическое выражение, которое, в свою очередь, формирует систему виртуальных следов этого деяния.

ЭЦИ о событии хулиганства в виде фотографий и видеофайлов, как правило, создается при помощи девайсов преступников или очевидцев хулиганства и сохраняется в виртуальном пространстве либо передается (распространяется) через мессенджеры, т. е. ПО или web-сервисы, предназначенные для мгновенного обмена сообщениями. Изучение уголовных дел о хулиганстве, возбужденных в 2012–2019 гг., позволяет отнести к наиболее популярным среди белорусских преступников такие мессенджеры, как Viber и WhatsApp.

Бывают случаи, когда группа хулиганов осуществляет публичную онлайн-трансляцию своих хулиганских действий, например, массового хулиганства фанатов одной из играющих команд в ходе спортивного мероприятия (футбольного или хоккейного матча). Возможность потоковой трансляции событий криминального хулиганства в режиме реального времени доступна благодаря мобильным видеостриминговым сервисам. Важной в криминалистическом аспекте является доступность для просмотра потоковых данных в течение 24 часов как при

помощи приложений, установленных в используемом девайсе, так и в браузере на сайте самого сервиса. Наиболее часто при совершении группового хулиганства преступники используют такие сервисы, как YouTubeLive и «ВКонтакте». Так, совершение в январе 2016 г. групповых хулиганских действий несовершеннолетними С., Н. и иными лицами, сопровождавшихся погромом в арендуемой на сутки квартире в г. Минске и повреждением чужого имущества, транслировалось онлайн на сервисе YouTubeLive.

Интернет активно применяют современные хулиганы для достижения целей по внесению в сознание других людей представления об их значимости, подтверждения причастности к определенной асоциальной группе, самовыражения, демонстрации процесса совершения хулиганских действий (независимо от форм их проявления) и получения ответной реакции в виде лайков или дизлайков. Соответственно, в виртуальном пространстве остаются следы таких действий, как в виде видеофайлов, так и текстовых файлов (электронная переписка в мессенджерах, на страницах социальных сетей или посты на выложенную в общий или приватный доступ видеозапись хулиганства). Например, хулиганские действия двух анархистов, выразившиеся в поджоге с использованием «коктейля Молотова» в июле 2017 г. в г. Ивацевичи билборда с изображением сотрудника милиции и надписью «Сила закона в его исполнении», были записаны на девайс пособника и выложены через социальную сеть и YouTube-канал для публичного просмотра.

Современные возможности интернета позволяют не только обеспечить дистанционную коммуникацию и создавать чаты, мессенджер-группы по интересам для обмена информацией в любой форме. Стремительно развивающиеся технологии являются удобным средством для размещения различного рода контента, в том числе видеофайлов с записью планирования или совершения хулиганских групповых действий. Такое использование технологий позволяет современным хулиганам существенно усилить эффект от их преступления, распространить информацию о нем, не ограничивая круг лиц. Наряду с мессенджерами и социальными сетями ими используется *видеохостинг*. При этом большинство подобных сервисов не предоставляют видео, следуя таким образом принципу «контент генерирует пользователь» (User-generated content). Наиболее популярными среди преступников являются YouTube (для загрузки видео нужно зарегистрироваться, а размер загруженных файлов не должен превышать 1Gb), видеопортал RuTube и сайт Vimeo.com.

Кроме того, ЭЦИ о хулиганстве может быть аккумулирована в виртуальном пространстве в виде видеофайлов, сохраняемых на серверах или ЦОДах камер видеонаблюдения, установленных в целях обеспечения общественной безопасности и охраны правопорядка. Например, с мая 2019 г. в Республике Беларусь функционирует республиканская система мониторинга общественной безопасности, разработанная в соответствии с Указом Президента Республики Беларусь от 25 мая 2017 г. № 187. В основу работы системы заложена технология KIPOD, которая позволяет вывести на новый уровень возможности белорусских правоохранителей по анализу Big Data и видеоконтента.

В контексте расследования хулиганства виртуальные следы представлены в виде ЭЦИ о событии хулиганства, находящейся в виртуальном пространстве, которая имеет доказательственное значение независимо от того, содержится ли она на определенном материальном (физическом) носителе и воспроизведена ли она в форме, доступной для визуального (аудиовизуального) восприятия.

Таким образом, к наиболее типичным местам обнаружения виртуальных следов по уголовным делам о хулиганстве относятся карты памяти и ПО девайса (в основном смартфонов), гаджеты, т. е. технические устройства, предназначенные для хранения ЭЦИ, в том числе флеш-накопители, ОЗУ ПК, винчестер ПК, создающий копию смартфона, ЦОДы и Дата-центры социальных сетей, мессенджеров, видеостриминговых сервисов.

УДК 342.9

М.В. Губич, кандидат юридических наук, временно исполняющий обязанности по должности заместителя начальника кафедры правовой информатики Академии МВД Республики Беларусь
gubichmv@yandex.by;
А.Ю. Богданкевич, курсант учебной группы 6112 4 «Б» курса факультета милиции Академии МВД Республики Беларусь
andreibogdankevitch@yandex.by

НАПРАВЛЕНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТ И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Цифровые технологии – неотъемлемая составляющая активности современного человека, организации, юридического лица. Их развитие происходит столь стремительно, что право не всегда успевает оперативно реагировать на появление новых технологических решений. По экспертным оценкам, по состоянию на середину октября 2019 г. капи-

тализация всех криптовалют составила более 220 млрд долл. США, что не могло не обусловить популярность цифровых активов как объекта научных исследований. Существует целый ряд технических качеств, с регулированием которых ранее не сталкивалась правовая наука: технологии распределенных реестров, безвозвратность проведенных операций (транзакций), отказ от централизованного хранения данных на серверах, возможность заключения и ведения смарт-контрактов непосредственно между сторонами при отсутствии посредников, возможность круглосуточного функционирования системы.

Указанные возможности не остались незамеченными криминалитетом. Так, по ряду экспертных оценок, в 2018 г. объем криминальных сделок, совершенных с использованием только лишь одной криптовалюты биткоин составил примерно 76 млрд долл., при этом основными направлениями криминального использования криптовалюты (в соответствии с отчетом Европола за 2018 г.) выступали:

незаконный оборот наркотических средств и психотропных веществ (применение теневых интернет-сервисов, продажа «химических конструкторов», позволяющих покупателю самостоятельно изготавливать наркотики);

отмывание преступных доходов (развитие нелегальных сервисов по конвертации криптовалюты и обналичивания фиатных средств, использование «программ-смесителей», которые позволяют запутать историю транзакций, отмывание через сайты азартных игр, использование криптовалюты при финансировании терроризма и т. д.);

корыстные преступления, где виртуальная валюта является предметом преступного посягательства (использование фейковых (поддельных) электронных кошельков, создание фишинговых сайтов (или сайтов-копий) популярных ресурсов, запуск краудинвестинговых проектов и инвестиционных фондов, собирающих средства в криптовалюте).

Необходимо акцентировать внимание на тенденции расширения спектра используемых в криминальных целях криптовалют. Если ранее в качестве абсолютного монополиста крипторынка выступал биткоин, то сейчас в криминальных сделках все чаще стали применяться валюты с высокой анонимностью (ZCash, Dash, Monero).

Популярность использования криптоалгоритмов в криминальной среде объясняется тем, что до настоящего времени не выработаны четкие правовые параметры криптовалюты и не установлены границы ее безопасного оборота.

С учетом международного и организованного характера компьютерной преступности в целом все обозначенные криминальные направления использования криптовалют характерны и для Республики Беларусь, в которой законодательное регулирование использования данных финансовых инструментов находится только на начальной стадии ста-

новления. В этой связи отечественному законодателю и правоохранительным органам необходимо выработать стандарты и методики противодействия указанным преступлениям, разработать такую модель правового регулирования оборота криптовалюты, в которой были бы решены задачи предупреждения совершения корыстных преступлений и поддержки инновационного развития экономики Беларуси.

Следует отметить, что с принятием Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» наша страна стала одним из лидеров в правовом регулировании порядка обращения криптовалюты, при этом определение Парка высоких технологий в качестве уполномоченного субъекта реализации норм данного документа имеет, несомненно, положительное значение в администрировании технологии реестра блоков транзакций, а также иных технологий, основанных на принципах распределенности, что позволяет национальным участникам отношений в рассматриваемой сфере совершать операции с использованием указанных технологий с большей степенью безопасности.

В настоящее время разрабатывается ряд проектов нормативных правовых актов в данной сфере, в том числе проект Декрета Президента Республики Беларусь, направленный на развитие действующего Декрета «О развитии цифровой экономики», что свидетельствует о реакции государства на развитие цифровой экономики и криптовалюты.

Однако, несмотря на предпринятые государством шаги, представляется необходимым выделить следующие перспективные направления правового регулирования рассматриваемых финансовых инструментов, что позволит как участникам операций и их использованием пребывать в большей безопасности, так и правоохранительным органам с большей результативностью противодействовать преступлениям, совершаемым с использованием криптовалют.

1. Определение единой международной правовой позиции относительно правовой сущности криптовалют, т. е. решение вопроса могут ли они быть включены в состав денежной массы или нет. В настоящее время существуют два основных мнения: виртуальные валюты не рассматриваются как формы денег, несмотря на наличие признаков, сходных с признаками денежных средств или электронных денег; криптовалюты должны быть приравнены к объектам гражданских прав с одновременным определением в специальных нормативных правовых актах пределов безопасности использования модели коллективного инвестирования (краудфандинга).

В рамках решения указанного вопроса необходима выработка и установление единого режима конвертации всех видов криптовалют в фиатные эквиваленты.

2. В целях противодействия рассматриваемым криминальным проявлениям необходимо установление обязательной идентификации владельцев криптовалюты и иных лиц, участвующих в ее обороте.

3. С учетом приведенных и иных примеров использования рассматриваемых финансовых инструментов в преступных целях полагаем необходимым введение ответственности за нарушение стандартов оборота криптоинструментов, а также создание открытой международной базы данных о лицах, допускающих такие нарушения.

Таким образом, криптовалюта является относительно новым и наиболее активно развивающимся элементом цифровой экономики, что объективно обусловило ряд проблемных вопросов, связанных с правовым регулированием ее оборота, в том числе организации эффективного противодействия криминальному использованию рассматриваемого финансового инструмента. При этом основными вопросами в правовом регулировании являются определение единой международной правовой позиции относительно правовой сущности криптовалюты, установление механизмов идентификации владельцев криптовалюты и иных лиц, участвующих в ее обороте, а также ответственности за нарушения стандартов оборота криптоинструментов.

УДК 342.9

М.В. Губич, кандидат юридических наук, временно исполняющий обязанности по должности заместителя начальника кафедры правовой информатики Академии МВД Республики Беларусь
gubichmv@yandex.by

СИСТЕМА СУБЪЕКТОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ И ИХ КОМПЕТЕНЦИЯ

Концепцией национальной безопасности Республики Беларусь и принятой в ее развитие Концепцией информационной безопасности определены основные функции системы обеспечения национальной безопасности, выполнение которых предполагает дальнейшее совершенствование имеющихся подсистем и механизмов, обеспечивающих надежность и устойчивость ее функционирования. Одним из направлений указанной деятельности является совершенствование деятельности субъектов противодействия компьютерным преступлениям.

Данные нормативные правовые акты закрепляют необходимость решения задач обеспечения национальной безопасности на основе системного подхода, в том числе посредством реализации комплекса

взаимосвязанных мер, направленных на выявление, предупреждение и нейтрализацию внутренних и внешних рисков, вызовов и угроз безопасности. Исключительно важную роль для обеспечения эффективности функционирования указанных субъектов играет их правильная, научно обоснованная организационная структура – система субъектов обеспечения информационной безопасности, а также противодействия преступления в сфере высоких технологий – как ее подсистема.

Следует указать, что субъекты, вовлеченные в рассматриваемую деятельность, многочисленны и разнообразны: граждане Республики Беларусь, иностранные граждане, общественные объединения, юридические лица; органы государственного управления, их структурные подразделения, должностные лица, которые наделены определенными полномочиями в данной сфере. Такая многосубъектность обусловлена комплексным характером противодействия преступлениям в сфере высоких технологий.

Защита жизни, здоровья, чести, достоинства, прав, свобод и законных интересов участников общественных отношений от преступных и иных противоправных посягательств относится к важнейшим функциям государства. Решение наиболее важных, основных вопросов в правоохранительной сфере входит в компетенцию органов государственного управления. Рассматривая деятельность Президента Республики Беларусь, Совета Безопасности Республики Беларусь, Национального собрания Республики Беларусь, Совета Министров Республики Беларусь в сфере противодействия компьютерным преступлениям, необходимо учитывать, что рассматриваемая система является подсистемой более высокого уровня – национальной безопасности. В этой связи решение вопросов противодействия преступлениям в сфере высоких технологий указанными субъектами осуществляется, как правило, в комплексе вопросов в сфере национальной безопасности.

Президент осуществляет общее руководство системой обеспечения национальной безопасности путем реализации своих полномочий в этой сфере через Совет Безопасности Республики Беларусь и его рабочий орган – Государственный секретариат Совета Безопасности Республики Беларусь, а также через Совет Министров Республики Беларусь. Президент Республики Беларусь определяет основные направления деятельности государства по защите жизненно важных интересов личности, общества и государства от внешних и внутренних угроз, осуществляет функцию координации деятельности по обеспечению национальной безопасности, в том числе противодействия преступлениям в сфере высоких технологий. Указанный элемент рассматриваемой системы является ее стратегическим центром, что позволяет ему эффективно выполнять возложенные на него задачи.

Совет Безопасности Республики Беларусь – высший коллегиальный координационно-политический орган, созданный в целях реализации полномочий Президента Республики Беларусь в области обеспечения национальной безопасности. Исходя из изложенного он наряду с Главой государства занимает центральное место в системе субъектов обеспечения национальной безопасности.

Система органов исполнительной власти во главе с Советом Министров Республики Беларусь осуществляет функции по непосредственному обеспечению национальной безопасности. Основная задача Совета Министров как субъекта противодействия преступлениям в сфере высоких технологий состоит в непосредственной реализации на надведомственном уровне стратегических решений, принятых Президентом Республики Беларусь и Советом Безопасности Республики Беларусь, а также организации выполнения требований нормативных правовых актов в сфере информационной безопасности.

Министерства и государственные комитеты Республики Беларусь согласно законодательству Республики Беларусь, реализуя задачи, возложенные на них, участвуют в обеспечении различных аспектов противодействия преступлениям в сфере высоких технологий в соответствии со своей компетенцией. Руководствуясь законами, декретами, указами, распоряжениями Президента Республики Беларусь, постановлениями Правительства Республики Беларусь, они реализуют политику государства, направленную на защиту жизненно важных интересов объектов безопасности, в том числе кибербезопасности. В этой связи органы исполнительной власти также являются компонентом рассматриваемой системы субъектов.

Национальное собрание Республики Беларусь осуществляет законодательное регулирование исследуемой деятельности, придает деятельности элементов системы правовой характер, устанавливает правовые пределы такой деятельности, посредством издания законов формирует формальное правовое единство целей, задач и полномочий, правовую общность элементов системы.

Судебные органы как элемент системы оценивает с позиции права те либо иные явления, негативно воздействующие на состояние информационной безопасности, и принимает решение о привлечении виновных в нарушении правовых норм, к установленной законом ответственности.

Прокуратура Республики Беларусь координирует правоохранительную деятельность государственных органов, осуществляющих противодействие преступлениям в сфере высоких технологий, а также осуществляет надзор за точным и единообразным исполнением законодательства.

К негосударственным субъектам противодействия преступлениям в сфере высоких технологий относятся юридические лица, общественные формирования, содействующие органам правопорядка. Данные

элементы системы можно рассматривать как вспомогательные элементы системы, выполняющие функции по непосредственному воздействию на внешнюю среду, что не снижает их значимости в обеспечении функционирования всей системы субъектов. Граждане также могут рассматриваться в качестве субъектов рассматриваемой системы. Основная роль граждан в указанной сфере состоит в создании благоприятных условий выполнения государственными субъектами возложенных на них задач, в том числе оказание разносторонней помощи путем сообщения правоохранительным органам о ставших им известными фактах готовящихся, совершаемых или совершенных правонарушений, причинах и условиях, способствующих их совершению, и т. п.

На основании вышеизложенного можно заключить, что противодействие преступлениям в сфере высоких технологий в большей либо меньшей степени составляет компетенцию всех без исключения государственных субъектов противодействия преступлениям в сфере высоких технологий, а также может осуществляться и негосударственными субъектами. При этом для их классификации, а также выявления закономерностей во взаимосвязях отдельных субъектов применимы общепринятые критерии классификации, разработанные административно-правовой наукой: территориальный масштаб деятельности, основания образования, объем и характер компетенции, порядок решения подведомственных вопросов, конкретная направленность компетенции, источник финансирования, место в системе органов власти и организационно-правовая форма.

УДК 343.98

В.В. Гулевич, курсант Академии МВД Республики Беларусь
gulevich_viktoriya.ru@mail.ru;
Р.М. Ропот, кандидат юридических наук, доцент кафедры криминалистических экспертиз следственно-экспертного факультета Академии МВД Республики Беларусь
r.r.m.86@mail.ru

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ СУДЕБНОЙ ЭКСПЕРТИЗЫ В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Неотъемлемым атрибутом современного общества является всеобъемлющий характер проникновения информационных технологий во многие сферы деятельности человека – социальную, финансовую, управленческую и др. Компьютер стал незаменимым элементом рабо-

чего стола как руководителей, так и рядовых сотрудников практически во всех направлениях жизнедеятельности. Сегодня можно с уверенностью утверждать, что если раньше темпы развития человечества определялись доступной ему энергией, то теперь – доступной информацией, при этом, невзирая на явные преимущества и достижения, информатизация явилась причиной множества негативных тенденций, обусловивших использование компьютерных средств в противоправных целях. Криминальная среда повсеместно «вооружилась» современными достижениями информационных технологий не только с целью совершения «высокотехнологичных» преступлений, но и для обеспечения механизмов самой преступной деятельности, формирования новых подходов в конспирации, оказания активного противодействия правоохранительным органам.

Изучение опыта борьбы с компьютерной преступностью однозначно позволяет заключить, что получение значимой с криминалистической точки зрения информации по преступлениям данной категории являются в должной степени эффективными только при условии повсеместного применения специальных знаний, областью изучения которых являются информационные технологии. В качестве одной из основных и наиболее распространенных форм использования специальных знаний в данном направлении выступает назначение и проведение судебных компьютерно-технических экспертиз (СКТЭ). В настоящее время эта область судебно-экспертной деятельности представляет собой уже сложившийся отдельный род исследований, которые проводятся для установления особенностей и признаков компьютерного (цифрового, программного, сетевого) объекта, выявления и изучения соответствующей следовой картины в расследуемом событии, а также получения доступа к информационным ресурсам, хранящимся на носителях данных, с последующим ее полноценным исследованием.

Наиболее распространенными объектами СКТЭ, как правило, выступают следующие: персональные компьютеры (ноутбуки, нетбуки и т. п.); разнообразные носители данных; периферийные электронные устройства; средства сетевой компьютерной связи; всевозможные комплектующие и компоненты указанных выше компьютерных средств (системные блоки, сервера, жесткие диски, платы памяти и др.); программное обеспечение, включая сами алгоритмы, а также первоначальные (исходные) тексты программ; электронные документы; файлы мультимедиа и пр.

Основными видами СКТЭ являются:

1) Аппаратно-компьютерная экспертиза, которая назначается и проводится в тех случаях, когда необходимо определить свойства и признаки (характеристики, параметры) компьютерно-аппаратных средств для установления обстоятельств, детерминированных закономерностя-

ми их функционирования. Задачами указанного экспертного направления выступают:

установление назначения и функций объекта как компьютерного средства, определение той роли, которую этот объект занимал;

определение типа (вида, модели), свойств и технических характеристик компьютерных средств;

диагностика технической исправности и определение состояния компьютерных средств, поиск в них отклонений (дефектов) от параметров, установленных предприятием-изготовителем, и пр.

2) Программно-компьютерная экспертиза, которая направлена на установление закономерностей создания (разработки), функционирования и изменения программного обеспечения (ПО). Данный вид СКТЭ решает следующие задачи:

определение установочных характеристик, параметров и функционального назначения (системного, прикладного) ПО, а также типов поддерживаемых аппаратно-программных платформ;

изучение функциональных алгоритмов и структурных особенностей ПО;

определение базовых характеристик, которым должна отвечать операционная система;

установление функций и свойств ПО, определение временных параметров его инсталляции;

диагностика фактического состояния исследуемого ПО, состава и параметров входящих в его содержание файлов (атрибуты, дата инсталляции и изменения), способов ввода-вывода данных, наличия (отсутствия) каких-либо отклонений от заданных требований (параметров);

выявление возможных изменений, которым могло быть подвергнуто ПО после его инсталляции.

3) Информационно-компьютерная экспертиза, предмет которой состоит в обнаружении, анализе и оценке информации, подготовленной пользователем или созданной ПО с целью обеспечения функционирования информационных процессов в компьютерной системе. Задачами такой экспертизы являются:

установление вида и содержания информации (данных);

диагностика состояния информации, выявление наличия в ее содержании непредусмотренных первоначальным назначением данных (нарушений целостности, вредоносных элементов);

определение первоначального содержания информации, подвергшейся изменению;

определение обстоятельств и условий внесения изменений в содержание информации;

установление последовательности и механизма развития расследуемых событий, обусловленных порядком создания, обработки, изменения и сохранения данных;

определение хронологических характеристик воздействия на информационные массивы;

установление пользовательских и профессиональных особенностей создателя (автора, разработчика) информации;

установление взаимообусловленности (причинной связи) между какими-либо конкретными действиями с информацией и наступившими последствиями и пр.

4) Компьютерно-сетевая экспертиза, предметом изучения которой выступают компьютерные системы и средства, обеспечивающие реализацию сетевых информационных технологий. Задачами в указанном направлении исследований выступают:

установление фактов и возможности использования тех или иных компьютерных средств для выхода в сеть Интернет;

обнаружение и анализ реквизитов, необходимых для доступа к сетевым ресурсам;

изучение журналов (протоколов) работы ПО, предназначенного для работы в сети Интернет;

установление данных сетевых соединений;

установление содержания сетевых сообщений и пр.

Вышеизложенное подтверждает, что судебная компьютерно-техническая экспертиза в состоянии решать различные задачи, которые, несомненно, являются востребованными при расследовании преступлений в сфере высоких технологий. Использование возможностей специальных знаний в данной области может являться не только значимым источником вещественных доказательств, но и выступать неотъемлемым атрибутом повышения эффективности борьбы с компьютерной преступностью.

УДК 159.9; 343.9

А.В. Ивановский, доктор технических наук, профессор, профессор кафедры правовой информатики Академии МВД Республики Беларусь
a_ivanovsky@mail.ru

МОДЕЛИРОВАНИЕ ПРОЦЕССА ФОРМИРОВАНИЯ ДЕСТРУКТИВНОЙ ИНФОРМАЦИОННОЙ ВОЙНЫ

Геополитические конкуренты активно используют информационное пространство для ведения политической (иные термины: идеологической, социально-политической, информационной) войны с помощью деструктивных информационно-психологических воздействий (ДВ).

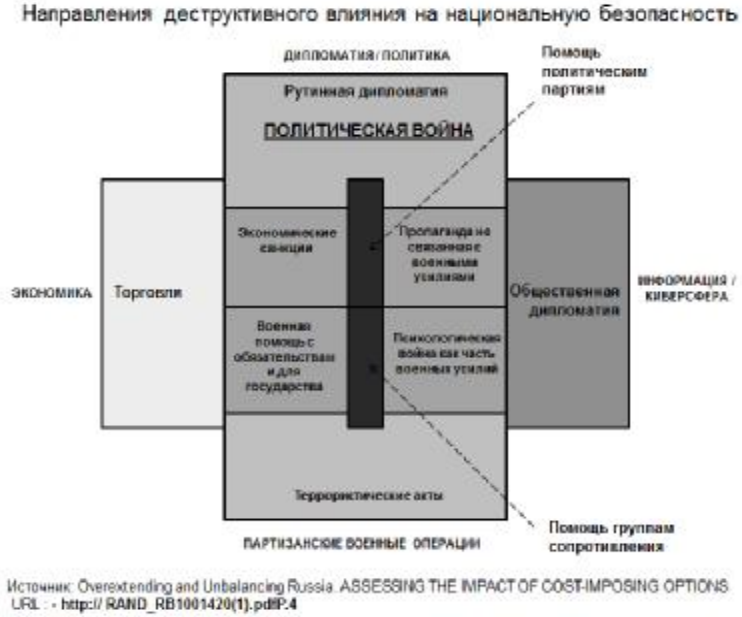


Рис. 3. Системный порядок формирования зон противоборства

В Концепции информационной безопасности Республики Беларусь, утвержденной Президентом Республики Беларусь А.Г. Лукашенко 18 марта 2019 г., содержательное наполнение термина ДВ отражает весь спектр угроз, возникающих при ведении социально-политической войны (рис. 3).

Объектом приложения ДВ в первую очередь является *морально-психологическое состояние общества,* которое определяется его восприятием сложившейся ситуации и национальным духом (менталитетом). Исследуя структурные элементы национального менталитета, А.В. Юревич выделил его ядерный слой, ключевые элементы: коллективную память; социальные представления, установки и отношения; закрепляющие их коллективные эмоции, чувства и настроения; нормы, ценности и идеалы; национальный характер и темперамент; язык; ментальные репрезентации культуры; стиль мышления и социальное восприятие; поведенческие образцы; национальную идентичность. На изменение этих элементов и ориентировано ДВ.

Изменение менталитета граждан и общества – процесс длительный. Для форсированного сокращения времени достижения целей информационного противоборства интервенты используют *технологию «окон*

Овертона». В технологии «окно» отражает смыслы и установки, в которые верит общество в данный исторический период. Содержание данных смыслов пытаются изменить с помощью ДВ, при этом распространяемые информационные материалы содержат как правдивые факты, так и недостоверную информацию. Такой способ информирования сопровождает «распад истины». В основе способа лежит гипотеза о том, что ДВ отражают новую картину мира и человек может изменить свои прежние установки, если они начинают не совпадать с реальностью. Факт изменения установок и смыслов отражает сдвиг «окна». Технически формируется и в сознание общества внедряется последовательность мэмов, создающая канву для поэтапной подмены смыслов и установок, закрепления новых ценностей, выгодных интервенту (https://www.mackinac.org/OvertonWindow).

При оценке информационной обстановки в Белнет можно контролировать ход компании путем оценки состояния ресурсов, структуры и параметров ДВ. Ход компании включает ряд этапов:

1. Выбирается главная цель и дерево дополнительных целей компании. Для достижения главной цели интервент системно концентрирует разнородные ресурсы и координирует их применение из единого центра. В состав компании включаются операции, направленные против страны-мишени. Их стержнем являются «окна Овертона».

2. В экономике, политической и общественной дипломатии, партизанских операций формируются зоны легального и нелегального противоборства. Помощь оказывается оппозиционным политическим партиям и группам сопротивления власти. На рис. 3 первые обозначены квадратами, а вторые – прямоугольниками. Эти группы поддерживаются организационным, финансовым, информационным, идеологическим, креативным и программно-техническим видами обеспечения.

3. Интервент формирует группировку, продвигающую и закрепляющую в обществе смыслов и установок, в которых заинтересованы организаторы ДВ. В состав группировки входят СМИ (зарубежные, национальные, региональные, ТВ-каналы, радио, газеты, интернет-СМИ); социальные медиа (группы, каналы, целевые социальные сети, блогеры, тролли); аналитические центры (экспертные сообщества, социологические службы, институты памяти, комитеты избирателей); оппозиционные власти организации (ассоциации, общественные объединения, профсоюзы, движения, различные платформы).

4. Для глубинного проникновения и токсичного влияния на общество используют агентов влияния в институтах государства: парламенте (депутаты, партии, партийные площадки); органах государственного управления (суды, исполнительная власть); силовых структурах (КГБ,

МВД, МЧС, армия); образовании (программы, обмены, гранты); культуре (музыканты, художники, писатели, деятели кино), спорте (фанаты, спортклубы). Дополнительно подключают зарубежный блок (договора, зарубежные НКО, делегации, дипломаты); фонды (международные, национальные, региональные); знаменитостей (актеры, спортсмены, музыканты и пр.); правозащитников (активисты, организации, международные структуры).

5. С помощью ДВ оказывается токсичное влияние на граждан и их группы. Кроме того, осуществляется оценка результативности проводимой работы.

Страна-мишень защищает свои национальные интересы, в первую очередь правовыми методами. В белорусском законодательстве введена *ответственность* за противоправную деятельность, обусловленную ДВ:

деструктивная пропаганда – ст. 123 (Пропаганда войны), ст. 130 (Разжигание расовой, национальной, религиозной либо иной социальной вражды или розни) Уголовного кодекса Республики Беларусь (УК);

призывы и иное побуждение к совершению преступлений и антисоциальных деяний – ст. 146 (Склонение к самоубийству), ст. 361 (Призывы к действиям, направленным на причинение вреда национальной безопасности Республики Беларусь) УК;

распространение ложной информации – ст. 188 (Клевета), ст. 367 (Клевета в отношении Президента Республики Беларусь), ст. 250 (Распространение ложной информации о товарах и услугах), ст. 257 (Обман потребителей), ст. 340 (Заведомо ложное сообщение об опасности), ст. 350 (Модификация компьютерной информации), ст. 369^1 (Дискредитация Республики Беларусь), ст. 400 (Заведомо ложный донос), ст. 401 (Заведомо ложное показание) УК;

сокрытие общественно важной информации – ст. 268 (Сокрытие либо умышленное искажение сведений о загрязнении окружающей среды) УК;

публичные оскорбления, унижение чести и достоинства – ст. 189 (Оскорбление), ст. 368 (Оскорбление Президента Республики Беларусь), ст. 369 (Оскорбление представителя власти) УК.

Как показала практика, эти нормы оказывают свое сдерживающее воздействие на организаторов и проводников ДВ.

УДК 343.97

П.А. Капіца, магістр юрыдычных навук, старшы следчы, Ленінскі (г. Мінска) раённы аддзел Следчага камітэта Рэспублікі Беларусь
p.kapitsa@sledcom.by

АБ ПРАБЛЕМАТЫЦЫ ВЫКАРЫСТАННЯ СПЕЦЫЯЛЬНЫХ ВЕДАЎ ПРЫ РАСКРЫЦЦІ І РАССЛЕДАВАННІ РАСКРАДАННЯЎ У СФЕРЫ ІНФАРМАТЫЗАЦЫІ

У Рэспубліцы Беларусь у цяперашні час высокія тэхналогіі актыўна ўкараняюцца ў дзейнасць дзяржаўных органаў і арганізацый (далей – дзяржаўныя органы). Для іх праграмна-тэхнічнага забеспячэння выдаткуюцца значныя бюджэтныя грашовыя сродкі. Да распрацоўкі праграмных прадуктаў для патрэб дзяржаўных органаў прыцягваюцца спецыялісты з недзяржаўных суб'ектаў гаспадарання на адплатнай дагаворнай аснове. Прадмет такіх дагавораў даволі спецыфічны – стварэнне і ўдасканаленне камп'ютарных праграм. У такіх умовах узнікае рызыка крыміналізацыі сферы інфарматызацыі, а менавіта ўчынення раскраданняў бюджэтных сродкаў і карупцыйных злачынстваў. У гаспадарча-прававыя адносіны з дзяржаўнымі органамі могуць уваходзіць асобы, якія, наўмысна невыконваючы або неналежным чынам выконваючы прынятыя на сябе абавязкі па дагаворах аб распрацоўцы і ўдасканаленні праграмных прадуктаў, завалодваюць дзяржаўнымі грашовымі сродкамі. У выніку злачыннай дзейнасці такога віду бюджэтныя сродкі растрачваюцца, а праграмы інфарматызацыі застаюцца нерэалізаванымі.

Найважнейшай акалічнасцю, якая падлягае даказванню пры выяўленні, раскрыцці і расследаванні раскраданняў і карупцыі ў сферы інфарматызацыі дзяржаўных органаў з'яўляецца факт наўмыснага невыканання або неналежнага выканання гаспадарча-прававых абавязацельстваў. У сувязі з гэтым неабходна дакладна вызначыць, што распрацаванае праграмнае забеспячэнне з'яўляецца няякасным. Для вырашэння такой задачы следчаму (супрацоўніку органа дазнання) патрэбны спецыяльныя веды. Згодна з КПК Рэспублікі Беларусь яны могуць быць выкарыстаны пры выкананні асобных следчых дзеянняў (для ўдзелу выклікаецца спецыяліст) або пры прызначэнні экспертыз. На практыцы пры расследаванні злачынстваў віду, які разглядаецца, дадзеныя палажэнні могуць быць рэалізаваны або шляхам правядзення агляду з удзелам спецыяліста, або шляхам прызначэння экспертызы. Уяўляецца, што для высновы аб няякаснасці камп'ютарнай праграмы непасрэдна агляду (у дадзеным выпадку – камп'ютарнай тэхнікі або

матэрыяльнага носьбіту, на якой праграмны прадукт змяшчаецца) недастаткова. Гэта звязана з тым, што сама сутнасць агляду як следчага дзеяння не прадугледжвае магчымасці рабіць канкрэтныя высновы аб адпаведнасці (неадпаведнасці) уласцівасцей таго ці іншага аб'екту матэрыяльнага свету пэўным патрабаванням. А.В. Дулаў адзначаў, што «следчы агляд заключаецца ў непасрэдным выяўленні і даследаванні аб'ектаў, якія маюць значэнне для крымінальнай справы, з мэтай вывучэння іх прыкмет, уласцівасцей, стану і ўзаемаразмяшчэння». Гэта значыць, што падчас агляду магчыма толькі зафіксаваць і апісаць тыя ці іншыя прыкметы і ўласцівасці матэрыяльнага аб'екта. Напрыклад, у пратаколе агляду можна занатаваць, што запуск праграмы не адбываецца (без высноў аб тым адпавядае гэта тым ці іншым патрабаванням або не).

Найбольш верагоднай крыніцай доказаў у такім выпадку, на нашу думку, можна лічыць заключэнне эксперта. Толькі падчас правядзення экспертызы можна вызначыць адпаведнасць камп'ютарных праграмных прадуктаў пэўным патрабаванням і ўмовам, паставіўшы перад кампетэнтнай асобай (асобамі) адпаведныя пытанні, пры гэтым эксперт, адказваючы на пытанні, павінен спасылацца на сучасныя веды ў навуцы, тэхніцы.

Для вызначэння якаснасці праграмных прадуктаў пры прызначэнні адпаведных экспертыз варта ставіць наступныя пытанні: «Ці адпавядае распрацаваны (указаць суб'ект гаспадарання) паводле дагавора (указаць дату і нумар дагавора) праграмны прадукт (указаць назву або іншыя характарыстыкі) тэхнічнаму заданню на распрацоўку праграмнага прадукту?»; «Ці адпавядае распрацаваны (указаць суб'ект гаспадарання) паводле дагавора (указаць дату і нумар дагавора) праграмны прадукт (указаць назву або іншыя характарыстыкі) сучаснаму стану развіцця навукі і высокіх тэхналогій?». Пастаноўка менавіта другога пытання неабходна таму, што нядобрасумленныя выканаўцы могуць знаходзіцца ў змове з прадстаўнікамі заказчыка ад самага пачатку працэдуры дзяржаўных закупак і аказваць уплыў на распрацоўку «патрэбнага» тэхнічнага задання.

Сістэмай органаў, службовыя асобы якой упаўнаважаны на выкананне судовых экспертыз у Рэспубліцы Беларусь, з'яўляецца Дзяржаўны камітэт судовых экспертыз (ДКСЭ). Для зручнасці прызначэння следчымі і іншымі ўпаўнаважанымі асобамі экспертыз ДКСЭ ў 2016 г. выдадзены зборнік метадычных рэкамендацый, у якім выкладаецца, якія віды экспертыз могуць праводзіцца ў ведамстве, якія матэрыялы павінны накіроўвацца на даследаванне і на якія пытанні ўпаўнаважаны адказваць эксперты. Паводле выдання, даследаванне праграмных прадуктаў і камп'ютарнай тэхнікі праводзіцца падчас камп'ютарна-тэхнічных экспертыз. Аднак у прыкладах пытанняў на экспертызы і ў задачах, якія вырашаюцца пры правядзенні даследавання, адзначаныя вышэй пытанні

не фігуруюць. Гэта значыць, ДКСЭ ў цяперашні час экспертызы такога віду не праводзяцца.

У сувязі з гэтым узнікае праблема пошуку кваліфікаваных спецыялістаў, якіх згодна з нормамі КПК Рэспублікі Беларусь можна прыцягнуць да выканання неабходнай камп'ютарна-тэхнічнай экспертызы. Уяўляецца, што яна можа быць вырашана двума асноўнымі шляхамі: падрыхтоўкай экспертаў і адпаведных методык правядзення экспертыз у сістэме ДКСЭ або прыцягненнем IT-спецыялістаў з іншых арганізацый. Апошні варыянт хоць і з'яўляецца больш хуткім прымяняльна да расследавання асобнага злачынства, але з-за стратнасці (павінны выдаткавацца дадатковыя бюджэтныя грашовыя сродкі) і нерэгулярнасці (немагчымасць прыцягваць адпаведных спецыялістаў на пастаяннай аснове) найбольш прымальным з'яўляецца падрыхтоўка спецыялістаў у ДКСЭ. Пры гэтым не выключана правядзенне камісійнай экспертызы, заключэнне якой можа быць падрыхтавана сумесна супрацоўнікамі адпаведнага ведамства і іншых арганізацый.

Такім чынам, пры расследаванні раскраданняў у сферы інфарматызацыі дзяржаўных органаў важна даказаць факт няякаснасці распрацаванага праграмнага прадукту, неадпаведнасці яго тэхнічнаму заданню і сучаснаму стану развіцця навукі і высокіх тэхналогій. Для вырашэння гэтай праблемы патрэбны спецыяльныя веды ў галіне праграмавання. Найбольш эфектыўным спосабам іх выкарыстання з'яўляецца прызначэнне камп'ютарна-тэхнічнай экспертызы. Аднак крыміналістычныя даследаванні менавіта такога віду ў цяперашні час у ДКСЭ не праводзяцца, што патрабуе або прыцягнення кваліфікаваных асоб з іншых арганізацый, або падрыхтоўкі неабходных спецыялістаў і методык правядзення экспертыз у сістэме ведамства.

УДК 343.37 + 004

В.Ф. Кетурко, преподаватель кафедры
правовой информатики Академии МВД
Республики Беларусь
kit-bu@mail.ru

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ВЫЯВЛЕНИЯ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационных технологий в современном обществе позволило в достаточной мере облегчить большинство процессов жизнедеятельности. Большая часть населения Республики Беларуси использует различные мобильные приложения для оплаты банковских

услуг, общения и т. д. Тенденция развития современных информационных технологий во всех отраслях жизни общества является позитивным моментом, отвечающим требованиям времени.

Совершенствование компьютерной техники, программного обеспечения, увеличения скорости передачи информации в сети Интернет, перемещения в ней большого объема информации позволило не только благоприятно отразиться в социально-экономической сфере, но и привело к формированию такого явления, как киберпреступность.

Деятельность государства по обеспечению эффективной информационной безопасности позволила в марте 2019 г. принять и утвердить Концепцию информационной безопасности Республики Беларусь, которая широко рассматривает вопросы суверенитета страны, защиту конституционных прав граждан от преступлений в сфере высоких технологий.

В Республике Беларусь по сравнению с 2017–2018 гг. отмечается рост преступлений в сфере высоких технологий. Состояние криминогенной обстановки в январе – декабре 2018 г. по сравнению с 2017 г. свидетельствует о значительном увеличении (+53,0 %; с 3 099 до 4 741) количества зарегистрированных киберпреступлений, при этом число уголовно наказуемых деяний увеличилось во всех регионах Республики Беларусь.

Изучение статистических данных по преступлениям в сфере высоких технологий позволяет сделать вывод о том, что наметился рост заинтересованности криминального элемента к данному направлению. Значительное количество преступлений – хищения с банковских платежных систем. Однако следует отметить, что в последние годы активно используются схемы завладения имуществом путем обмана или злоупотребления доверием с использованием информационных технологий. В Республике Беларусь данные действия квалифицируются как мошенничество, закрепленные в ст. 209 (Мошенничество) Уголовного кодекса Республики Беларусь.

Несмотря на уменьшение количества мошенничеств в 2018 г. 4 156 мошенничеств (в 2017 г. – 4 823), отмечается их рост с использованием информационных технологий. Необходимо отметить, что по мошенничествам, совершаемым в сети Интернет, не проводят проверку подразделения по раскрытию преступлений в сфере высоких технологий, а рассматриваются подразделениями уголовного розыска.

Лицам, обладающим цифровыми компетенциями и возможностью доступа к информации любого свойства, открываются большие возможности использования ее в корыстных целях. Возможность преступника совершать преступления удаленно, без непосредственного контакта со своей жертвой в значительной степени затрудняет выявле-

ние и расследование таких противоправных деяний, обусловливая высокий уровень их латентности.

Интенсивность разработки схем мошенничеств, совершаемых при помощи информационных технологий, недостаточность опыта и сил в данном направлении борьбы с преступностью, еще не позволяет в достаточной мере противостоять данному виду преступлений.

Современные преступники, разрабатывая различные схемы совершения мошенничеств, совершаемых с использованием информационных технологий, используют достижения научно-технического прогресса, активно используются знания в области компьютерной техники и программирования. Для получения большей выгоды и применения более изощренных способов совершения мошенничеств криминальные субъекты объединяются в устойчивые преступные группы, носящих часто транснациональный характер, при этом жертвой преступных деяний может стать любое физическое или юридическое лицо, государственная и негосударственная организация.

В настоящее время оперативные сотрудники применяют рекомендации по выявлению мошенничества, которые по своей структуре сходны с мошенничествами, совершаемыми с использованием информационных технологий, однако имеют иную специфику. Данные обстоятельства определенным образом сказываются на снижении способности правоохранительных органов своевременно выявлять и раскрывать факты совершенного преступления.

Борьба с мошенничеством, совершенным с использованием информационных технологий, будет возможна лишь тогда, когда правоохранительные органы будут вооружены научными положениями и разработанными на их основе практическими рекомендациями по выявлению и расследованию данного вида преступлений.

Очевидно, что случаи мошенничества, совершенного с использованием информационных технологий, были зафиксированы и ранее, тем не менее совершалось оно не так часто, как в настоящее время. Различные исследователи осуществили попытки изучения данной темы, однако рассматривали только отдельные элементы проблем выявления мошенничеств, совершаемых с использованием информационных технологий. Таким образом, актуальность темы обусловливается рядом проблем теоретического и прикладного характера. В настоящее время необходимо решить много научно-практических задач совершенствования деятельности органов внутренних дел Республики Беларусь, направленных на выявление мошенничеств, совершенных с использованием информационных технологий:

требуется более полное изучение анализа правовых основ и современного состояния практики;

необходимо разработать криминалистическую характеристику данного вида преступлений;

рассмотреть способы совершения;

выделить организационные и тактические особенности;

разработать научно-практические рекомендации по проведению (организации) следственных действий, оперативно-розыскных и иных мероприятий при выявлении и раскрытии преступлений.

УДК 004 + 343

В.А. Кудинов, кандидат физико-математических наук, доцент, профессор кафедры информационных технологий и кибербезопасности Национальной академии внутренних дел (г. Киев, Украина)
kafedra@i.ua

СОВРЕМЕННЫЕ ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ АНАЛИЗА ЦИФРОВЫХ ФОТОГРАФИЙ, КОТОРЫЕ МОГУТ ИСПОЛЬЗОВАТЬСЯ В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

Сегодня мы наблюдаем высокий уровень использования гражданами возможностей современных информационных технологий в своей повседневной деятельности, в частности, активное создание ими цифровых фотографий и их публикацию в соцсетях, сохранение в своих средствах мобильной связи и вычислительной техники. Работники правоохранительных органов для эффективного противодействия компьютерной преступности могут использовать ряд современных программных средств для анализа цифровых фотографий, а именно: подлинности, даты, времени и месте создания, технического устройства съемки и сведений о человеке.

Цифровая фотография, по сути, – это программный файл, в котором, кроме информации о самом изображении, сохраняется информация о том, как оно было сделано. Эта информация называется метаданные фотографии. Метаданные размещаются в своих специальных разделах, как, например, «Свойства файла», EXIF, IPTC и других, необходимых при хранении фотографий. Метаданные фото – информация, полезная в обычном случае, но опасная для тех, кто хочет обеспечить себе максимальную анонимность. Так называемые EXIF-данные могут рассказать не только о параметрах фотоаппарата/смартфона, из которого бы-

ла сделана фотография, но и многое другое (дату создания, геолокацию, информацию о владельце фото и т. д.).

Существует множество способов выяснить EXIF-данные фотографии, независимо от того, кто ее владелец и где ее местонахождение. Среди этих способов наибольшей популярностью пользуются варианты с браузером, средствами Windows и онлайн-сервисами. Рассмотрим их более подробно.

1. *С помощью браузера*. Поиск информации по фотографии с помощью браузера, пожалуй, самый простой и доступный способ. Чтобы узнать нужные данные про фото, можно использовать: 1) для Google Chrome – нужно установить расширение Exponator или Exif Viewer; 2) для Internet Explorer – нужно скачать приложение IExif. После установки расширения достаточно лишь навести курсор на любое фото, чтобы получить необходимую информацию; 3) для Mozilla Firefox – браузер поддерживает удобные расширения Exif Viewer или FxIF для распознавания метаданных фото.

2. *С помощью средств Windows.* Необходимо кликнуть правой кнопкой мыши по фото, выбрать команду «Properties» и найти в окне вкладку «Details», где можно узнать параметры фото, ее геолокацию, дату и другие данные.

3. *С помощью онлайн-сервисов.* Они позволяют быстро узнать EXIF-данные фото. Достаточно лишь загрузить фотографию на сервис или указать прямую ссылку на нее, а все остальное он сделает сам.

Findexif.com – бесплатный сервис. Минимум функционала и простота в использовании (в нем нет возможности загрузить фотографии, сервис работает только со ссылками). Предоставляет EXIF-данные.

Fotoforensics.com – сайт, который может обнаружить error level analysis (ELA), т. е. «дорисованные» области на изображении или вставленные в него при редактировании. После обработки программа выдает фотографию, где редактируемые фрагменты будут выделяться на фоне других. Кроме того, программа также предоставляет EXIF-данные фотографии.

Jeffrey's Exif Viewer – бесплатный сервис, который позволяет определить происхождение фотографий и изображений. С его помощью можно узнать EXIF-данные. Преимущество сервиса в том, что он позволяет изучить изображение как по ссылке из сети Интернет, так и загрузив его с компьютера.

Google Search by Image – обратный поиск изображений: загрузив фото, можно отследить первоисточник, а также выяснить, где она еще публиковалась.

TinEye – этот инструмент работает по принципу Google Search by Image.

JPEGSnoop – программа, которая устанавливается на компьютер (работает только в Windows) и позволяет смотреть метаданные не только изображений, но и форматов AVI, DNG, PDF, THM. Программу можно использовать для многих целей: позволяет увидеть, редактировалось ли изображение, выявить ошибки в поврежденном файле и т. п.

Рассмотрим особенности установления места съемки. Если информация о геолокации есть в метаданных, то она может помочь с предельной точностью установить место съемки. Но в то же время наличие данных о геолокации зависит от нескольких факторов. Во-первых, от устройства, которым была сделана фотография. В некоторых камерах или мобильных устройствах может не быть GPS-датчика, который фиксирует координаты. Во-вторых, от желания пользователей мобильных устройств – они могут отключить геолокацию из соображений приватности или уменьшения нагрузки на аккумулятор. В-третьих, наличие таких данных зависит от ресурса, на котором фотография была опубликована. Социальные сети Facebook, Twitter или Instagram удаляют метаданные из самих фотографий во время загрузки на серверы этих ресурсов. Но в то же время они могут непосредственно показывать информацию о местонахождении автора фотографии, если он дал доступ к GPS-датчику своего мобильного устройства.

Иногда возникает необходимость в изменении EXIF-данных фото. Самый простой способ удалить скрытые данные в фото – использовать системные инструменты Windows. Для этого необходимо кликнуть правой кнопкой мыши по фотографии, выбрать команду «Properties» и найти в окне вкладку «Details». Кликнуть внизу пункт «Удаление свойств и личной информации». После этого на вкладке можно самостоятельно выбрать данные, которые нужно удалить. Если нежелательно потерять эти данные, то можно создать копию фотографии с удаленными EXIF-данных, сохранив при этом оригинал.

Наименее требователен к профессиональным навыкам способ – использовать онлайн-сервисы. Хорошим примером такого сервиса является *IMGonline*, который позволяет быстро выбрать нужные данные и заменить их необходимыми параметрами. Копирование всех встроенных метаданных из одной фотографии в другую происходит без сжатия и потери качества.

Таким образом, нами проведен анализ современных программных средств для анализа метаданных цифровых фотографий, которые могут использоваться в борьбе с компьютерной преступностью.

УДК 343.85

С.В. Кузьменкова, кандидат юридических наук, преподаватель кафедры правовой информатики Академии МВД Республики Беларусь
kuzmenkov-k@mail.ru

О ПРОФИЛАКТИКЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ НЕСОВЕРШЕННОЛЕТНИХ

Современное развитие научно-технического прогресса в Республике Беларусь обусловливает процесс совершенствования информационных технологий, представляющих большой интерес как в юридической науке, так и в общественной жизни. Нынешние компьютерные технологии имеют различные преимущества, но вместе с тем они способствуют созданию условий, которые благоприятствуют совершению компьютерных преступлений. Следует отметить, что киберпреступность – достаточно новый вид преступлений, характеризующийся большим разнообразием и изменчивостью в связи с непрерывным развитием информационных технологий и совершенствующимися возможностями сети Интернет. Основной интерес данных преступлений сосредоточен на информации, информационных ресурсах или технике.

В настоящее время количество преступлений в информационной сфере характеризуется неблагоприятными тенденциями, которые прослеживаются на общем фоне роста преступности не только среди взрослых, но и несовершеннолетних правонарушителей. Непрерывный технический прогресс достаточно быстро активизирует интерес детей и подростков в сфере компьютерных преступлений, которые являются одними из наиболее активных пользователей электронных устройств и сетевых ресурсов. Так, например, в 2017 г. в Республике Беларусь к уголовной ответственности за компьютерные преступления, совершенные несовершеннолетними, было привлечено 34 лица, 2018 г. – 35, а в начале 2019 г. данный показатель уже составил 9 несовершеннолетних.

Противоправное поведение несовершеннолетних давно считается важнейшей проблемой, требующей разрешения. Политика государства в отношении несовершеннолетних всегда отличалась особым подходом, связанным с заботой о детях и защитой детства. Законом Республики Беларусь «О правах ребенка» закреплены общие положения, связанные с защитой детей, в том числе в связи с совершением уголовно-противоправных деяний. В уголовно-правовом смысле дети, не достигшие 18-летнего возраста, имеют особый правовой статус в плане применения к ним уголовной ответственности.

Несовершеннолетние – еще не сформировавшиеся в полной степени молодые юноши и девушки, которым присущи определенные ошибки в выборе социально одобряемого поведения. Формирование личности несовершеннолетнего находится еще в стадии становления, развития, такие лица более подвержены влиянию со стороны старших по возрасту, чем взрослые, пытаются подчас подражать им своими действиями и поведением. Преступления в сфере компьютерной информации, совершаемые несовершеннолетними, – характерная черта современной преступности, требующая определенных подходов для ее предотвращения.

Уголовным кодексом Республики Беларусь (УК) предусмотрен ряд компьютерных преступлений, которые несовершеннолетние способны совершать, не владея при этом определенными знаниями в области программирования, а всего лишь основываясь на собственные навыки и техническую осведомленность в данной сфере. В последние годы правоприменительная практика свидетельствует о том, что в Республике Беларусь наиболее распространенным преступлением, которое совершается несовершеннолетними, является хищение путем использования компьютерной техники (ст. 212 УК), представляющее разновидность кражи, уголовная ответственность за которую наступает с 14 лет.

Многие западноевропейские государства в определенных случаях устанавливают уголовную ответственность за киберпреступления начиная с 14 лет. С 4 апреля 2016 г. вступившие в силу изменения и дополнения в УК предусматривают, в отдельных случаях, снижение возраста с 16 до 14 лет, с которого наступает уголовная ответственность за компьютерные преступления. Необходимо отметить, что подросток в возрасте 14 лет способен осознавать противоправность своих действий в сфере компьютерной информации. Учитывая современные возможности компьютерных технологий, их доступность, а также информационный интерес несовершеннолетних целесообразно скорректировать перечень статей, предусматривающих наступление уголовной ответственности за компьютерные преступления с 14 лет с целью недопущения пробелов в статистическом учете компьютерных преступлений.

Следует отметить, что значимая роль в предупреждении компьютерных преступлений несовершеннолетних отводится их родителям. Ведь именно они находятся в постоянном контакте со своими детьми. В свое время известный американо-канадский ученый в области информатики Ричард Холт справедливо подчеркнул, что «родителям необходимо знать круг общения своих детей и их активность в сети Интернет и в реальной жизни». Кроме этого, практика показывает, что существует связь между киберпреступлениями и низким уровнем самоконтроля школьников. По мнению Холта, для родителей это представляет большую сложность. «Эти дети импульсивнее, они более

склонны к риску; есть большая вероятность того, что они воспользуются выпавшей возможностью, – объяснил он. – Поэтому крайне важно понимать поведение своих детей».

Проведение профилактической работы среди несовершеннолетних сотрудниками образовательных учреждений весьма эффективно в отношении детей старшего школьного возраста, но несовершеннолетние, которые только знакомятся с глобальным информационным пространством, нуждаются в непрерывной индивидуальной работе со стороны своих родителей. Представляется, что для достижения успеха в вопросе недопущения совершения преступлений в информационной сфере несовершеннолетними особое значение имеет осведомленность родителей в данной области, установка доверительных отношений между родителями и детьми, а также использование специального программного обеспечения, позволяющего не только контролировать, но и ограничивать деятельность ребенка в сети Интернет и др. Очевидно, что контроль и подробное разъяснение ответственности за совершение противоправных деяний в информационной сфере, а также приведение действительных примеров, будет способствовать уменьшению количества совершения преступлений несовершеннолетними в данной области.

Таким образом, непрерывная и целенаправленная работа с несовершеннолетними является залогом успеха в профилактике совершения компьютерных преступлений подрастающим поколением. С целью объективного ведения статистического учета компьютерных преступлений, совершенных лицами моложе указанного возраста, правильнее было бы предусматривать уголовную ответственность за некоторые компьютерные преступления с наступлением частичной (неполной) дееспособности (лицо в возрасте 14 лет).

УДК 343.97

В.В. Лавренов, старший преподаватель
кафедры правовой информатики Академии
МВД Республики Беларусь
VicLavrenov@mail.ru

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ФАКТОРНОГО И КОРРЕЛЯЦИОННОГО АНАЛИЗА ПРИ ПОСТРОЕНИИ ЭФФЕКТИВНОЙ СИСТЕМЫ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Согласно Концепции информационной безопасности Республики Беларусь трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают

вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба), при этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

Математика, будучи абстрактной наукой, обладает универсальным характером, и потому ее достижения применимы ко многим отраслям знаний, в том числе и к общественным наукам, и к юриспруденции, особенно в тех областях, где возможен процесс формализации знаний, при этом следует отметить, что основным полем совершения преступлений в сфере высоких технологий является киберпространство, которое организовано и функционирует по строгим «законам математики». В этой связи для повышения эффективности борьбы с компьютерной преступностью, наряду с традиционными методами борьбы особую значимость приобретает познание закономерностей развития криминологических и социально-правовых явлений, основанных на применении научных методов исследования.

Все явления и процессы, связанные с компьютерной преступностью, находятся во взаимосвязи и взаимообусловленности. Одни из них непосредственно связаны между собой, другие косвенно. Важный методологический вопрос в современном мире – выявление, изучение и измерение факторов, влияющих на компьютерную преступность. При этом представляется, что наибольшим потенциалом в исследовании компьютерной преступности обладает факторный анализ, осуществляемый посредством эконометрической методики исследования, что позволяет научно обосновать стратегию и методику противодействия компьютерной преступности, а также прогнозировать ее уровень и те явления, которые ее порождают и обусловливают.

Указанная нами позиция основывается на том, что факторный анализ является апробированной наукой совокупностью методов и моделей, изучающих и объясняющих связи между наблюдаемыми количественными и качественными признаками, измеряющих степень влияния факторов на изменение результативного показателя. Говоря по другому, факторный анализ – это изучение взаимосвязи результата и факторов (причин).

Вместе с тем, как показывает практика применения теоретических конструкций, для достижения результата, позволяющего отобразить связи в реальной жизни с результатами теоретических расчетов необходимо применение корреляционного анализа – метода обработки статистических данных, с помощью которого измеряется теснота связи между двумя или более переменными, что особенно важно для исследования социальных явлений (в том числе преступности) и особенно в киберпространстве.

Корреляционный анализ тесно связан с регрессионным, с его помощью определяют необходимость включения тех или иных факторов в уравнение множественной регрессии, а также оценивают полученное уравнение регрессии на соответствие выявленным связям.

С помощью факторного анализа можно решить две основные задачи: сделать описание компьютерной преступности кратко и в то же время всесторонне. Используя факторный анализ можно выявить факторы, отвечающие за наличие связей между исследуемыми переменными. Указанное позволяет, например, при проведении аналитической работы, сопутствующей профилактике, раскрытию, расследованию компьютерных преступлений, анализировать оценки, полученные по нескольким шкалам, выявлять среди них сходные между собой и имеющие высокий коэффициент корреляции, что позволяет предполагать о существовании латентной переменной, с помощью которой можно объяснить наблюдаемое сходство полученных оценок. Такая латентная переменная и является тем фактором, который влияет на многочисленные показатели других переменных, что приводит к возможности и необходимости отметить его как наиболее общий, более высокого порядка. Таким образом, можно выделить две цели факторного анализа при исследовании преступлений в сфере высоких технологий:

определение взаимосвязей между переменными, их классификация, т. е. «объективная R-классификация»;

сокращение числа переменных.

Для выявления наиболее значимых факторов целесообразно применять метод главных компонентов. С помощью этого метода можно уменьшить размерность данных путем замены взаимосвязанных (коррелируемых) компонентов на не связанные факторы. Другой важной характеристикой метода является возможность ограничиться наиболее информативными главными компонентами и исключить остальные из анализа, что упрощает интерпретацию результатов.

Факторный анализ проводится в несколько этапов.

При проведении первого этапа осуществляется анализ проблемного поля в целях отбора факторов, например, обусловливающих совершение компьютерных преступлений. Второй заключается в классификации и систематизации указанных факторов. На третьем строится структура связей между результативным и факторными показателями. На четвертом проводится расчет влияния факторов и оценка роли каждого из них в изменении величины результативного показателя. Заключительным, пятым, этапом является использование факторной модели на практике.

Таким образом, с помощью факторного и корреляционного анализа из всей совокупности факторов можно выделить значимые факторы, которые достаточно точно влияют на компьютерную преступность. Для построения эффективной системы борьбы с компьютерной преступностью, выбора оптимальных мер ее профилактики требуется научное сопровождение, информационное обеспечение, важное место в котором принадлежит анализу факторов, способствующих негативным изменениям компьютерной преступности.

УДК 343.985

Д.Н. Лахтиков, кандидат юридических наук, доцент, начальник кафедры правовой информатики учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
dzymitriy@yandex.by

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

В настоящее время наблюдается устойчивый рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, при этом не только преступлений против информационной безопасности и хищений с использованием компьютерной техники, но более «традиционных», таких как мошенничества, вымогательства и др.

Проблема противодействия данным преступлениям привлекает все большее внимание исследователей различных отраслей научного знания, при этом необходимость противодействия данному виду преступ-

лений, обусловливает и актуализирует ряд проблемных вопросов, как теоретического, так и прикладного характера. К актуальным вопросам в этом направлении относятся такие как повышение оперативной осведомленности соответствующих субъектов, совершенствование поисково-аналитической работы, определение актуальных направлений исследований, подготовка кадров и др.

В противодействии преступности определенная роль отводится применению оперативно-розыскных мер, направленных на предупреждение, выявление и пресечение преступлений. Актуальность мер оперативно-розыскного характера обусловлена тайным характером преступлений, а применение негласных возможностей позволяет эффективно решать стоящие перед правоохранительными органами задачи. При осуществлении противодействия преступности возникает необходимость в высокой осведомленности органов внутренних дел, что, согласно практике оперативно-розыскной деятельности (ОРД), осуществить без помощи граждан затруднительно. Законодательство в сфере ОРД позволяет использовать возможности лиц, оказывающих содействие на конфиденциальной основе, с целью установления события преступления и лиц, причастных к его совершению, выявления особенностей преступной деятельности и решения других задач. В теории и практике ОРД и при осуществлении правоприменительной деятельности выделяется анонимное содействие, которое отдельные ученые относят к разновидности конфиденциального, другие – к самостоятельному виду содействия субъектам ОРД, отмечая, что анонимное содействие является отдельным видом содействия в ОРД, которое осуществляется путем анонимного предоставления информации, когда лицо, ее предоставляющее, не желает раскрывать свои персональные данные.

С учетом активной информатизации общества, активного развития информационно-коммуникационных технологий, анонимное содействие граждан в ОРД представляет определенный интерес для повышения осведомленности заинтересованных правоохранительных органов. Гражданин, не привлекая внимания, может с помощью находящегося при нем смартфона зафиксировать какое-либо событие и в минимальные сроки предоставить интересующимся субъектам, которыми могут выступать ОВД, либо с помощью специально созданного канала в распространенных мессенджерах передать информацию, представляющую интерес для решения задач, стоящих перед ОВД. В сети Интернет функционирует информационный ресурс Министерства внутренних дел Республики Беларусь, и обеспечение на его платформе современной возможности предоставления анонимной информации может способствовать повышению уровня непосредственного взаимодействия

между ОВД и гражданами (в лице пользователей сайта). Именно наличие такой возможности свидетельствует о том, что ОВД открыты для диалога с гражданами, готовы как для предоставления, так и восприятия информации, но уже на более высоком уровне, при этом коммуникация выстраивается с учетом простоты пользования, экономии времени за счет возможности предоставления информации в различном виде: фото, видео, звук, текст. Интересная организация такого канала в различных мессенджерах, которыми активно пользуются граждане (например, Telegram, Viber и др.).

В свою очередь, повышение роли информационно-коммуникационных технологий влечет появление новых способов связи, особое место среди которых занимает интернет, аккумулирующий в себе огромные возможности в сфере взаимодействия людей, сформировавшей особый тип коммуникационной среды. Смещение акцентов информационно-аналитической работы в сети Интернет позволяет расширять поле противодействия преступности. В настоящее время, когда практически любое учреждение (организация) в интернете имеет значительные информационные массивы, когда большинство граждан имеют страницы в социальных сетях, пользуются различными интернет-форумами, поиск в сети Интернет с последующим анализом становится неотъемлемым этапом информационно-аналитической работы, связанной противодействием преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Расширяющееся использование информационных технологий в различных сферах изменило представление о месте и роли информации, средствах ее обработки. Например, недопустимо игнорирование технологий аналитического поиска Data Mining, активно внедряемых во многие сферы жизни общества.

Совершенствование подготовки кадров для противодействия преступности тесно связано с научно-исследовательской деятельностью в этом направлении. Среди перспективных направлений научно-исследовательской работы в этой области можно обозначить следующие: исследования криминологической, уголовно-правовой, криминалистической и оперативно-розыскной направленности. Так, например, проблем уголовно-правового характера, касающихся преступлений, совершаемых с использованием информационно-коммуникационных технологий; различные аспекты организации и тактики осуществления ОРД в сети Интернет; поиск информации, представляющей интерес в сети Интернет; выявление и расследование кибермошенничеств и кибервымогательств; прикладные проблемы компьютерной разведки; различные аспекты идентификации пользователей в сети Интернет;

криминалистическое исследование цифровой информации; разработка методов поиска виртуальных следов в блокчейн-системах, составляющих основу функционирования криптовалютной индустрии, и др.

Таким образом, определяя возможные пути совершенствования деятельности по повышению осведомленности ОВД, необходимо отметить максимальное использование различных возможностей поиска носителей информации, а не ограничиваться уже известными алгоритмами получения оперативной информации. Возможность предоставления гражданами анонимной информации, в том числе с использованием информационно-коммуникационных технологий, должна способствовать совершенствованию информационного обеспечения ОВД, что позволяет создать новый канал получения оперативной информации, а также задействовать имеющиеся резервы повышения эффективности оперативно-розыскных мер в борьбе с преступностью, в том числе компьютерной.

Проведение комплексных научных исследований в рассматриваемом направлении открывает новые возможности для дальнейшего развития не только науки, но и образовательного процесса в области подготовки кадров для субъектов, осуществляющих противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

УДК 343.985.7

П.В. Лутович, преподаватель кафедры правовой информатики учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
lpv2222@mail.ru;
Н.И. Рудович, кандидат юридических наук, доцент учреждения образования «Белорусский государственный экономический университет»
Roodnik@mail.ru

ОТДЕЛЬНЫЕ АСПЕКТЫ СОТРУДНИЧЕСТВА ГОСУДАРСТВ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Развитие информационных технологий открывает новые возможности для решения многих традиционных и бытовых задач. Новые технологии не только облегчают жизнь простых граждан, но и способствуют созданию и производству высокотехнологичной, конкурентоспособной

продукции, пользующейся высоким спросом на международных рынках. Более того, с учетом современных тенденций развития трансграничных отношений в различных сферах экономического сотрудничества, вызванных созданием ряда межгосударственных объединений в рамках интеграционных процессов Республики Беларусь, объективно возникает необходимость совершенствования правового регулирования данной сферы общественных отношений.

В то же время инновационные процессы способствуют возникновению новых угроз незаконного характера, на которые соответствующие правоохранительные органы должны своевременно реагировать. В Бангкокской декларации от 23 апреля 2005 г. «Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия» отмечено, что быстрое развитие информационных технологий, новых телекоммуникационных систем и компьютерных сетей сопровождается злоупотреблением этими технологиями путем их применения в противозаконной деятельности, при этом уделено внимание не только необходимости своевременной разработки эффективных национальных мер, но и развитию международного сотрудничества в борьбе с преступностью в указанной сфере деятельности.

В современной науке международного права международное сотрудничество в борьбе с преступностью рассматривается как специальная деятельность государств (иных субъектов международного права) в сфере предупреждения (профилактики) преступности, борьбы с ней и обращения с правонарушителями. Практика борьбы с международной преступностью показывает, что если страна проводит эффективную политику противодействия преступности, используя более решительные меры по пресечению преступной деятельности, то преступные организации, как правило, переносят свой преступный бизнес в страну с более лояльным правовым режимом.

Механизм международного сотрудничества в борьбе с преступностью проявляется в двух основных формах (договорно-правовой и организационно-правовой). Договорно-правовой механизм сотрудничества государств в борьбе с преступностью рассматривается как сотрудничество государств в борьбе с различными видами международных преступлений и преступлений международного характера на основе международных договоров. Положения этих международных актов в первую очередь направлены на обеспечение неотвратимости уголовного преследования и наказания преступников, вина которых установлена соответствующими национальными судами на основе действующего национального уголовного законодательства.

Организационно-правовой механизм сотрудничества государств в борьбе с преступностью – сотрудничество государств в борьбе с раз-

личными видами международных преступлений и преступлений международного характера под эгидой (в рамках) международных организаций, органов, конференций, совещаний.

В этой связи следует отметить актуальность международного сотрудничества правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий. Несмотря на ряд принятых универсальных международных соглашений в указанной сфере деятельности, определяющую роль, по нашему мнению, в противодействии совершению преступлений с использованием информационных технологий в нашей стране играет организационно-правовой механизм регионального сотрудничества в рамках Содружества Независимых Государств (СНГ).

В условиях устойчивого роста преступлений в этой сфере на территории государств – участников СНГ наблюдается активизация взаимодействия правоохранительных органов стран СНГ по ряду направлений. Так, одобрены и активно реализуются Межгосударственная программа сотрудничества государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий на 2016–2020 годы; Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности от 10 октября 2008 г.; Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, от 25 октября 2013 г.; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г. и др.

Согласно вышеназванным документам противодействие преступлениям, совершаемым с использованием информационных технологий, обеспечивается:

путем обмена оперативной, статистической, научной, методической и другой информацией о состоянии преступности в сфере информационных технологий;

обмена информацией для пополнения единой базы данных о транснациональных преступных группах и преступных организациях, совершающих преступления с использованием информационных технологий;

проведения согласованных следственных действий, комплексных совместных или согласованных профилактических оперативно-розыскных мероприятий и специальных операций;

выполнения запросов от компетентных органов других государств – участников СНГ;

внедрения технологий, рекомендаций и согласованных мер, ограничивающих возможности совершения преступлений с использованием информационных технологий, и др.

В заключение следует отметить, что появление новых криминальных вызовов и угроз требует разработки повышенных требований к состоянию правопорядка и объективно обусловливает необходимость своевременной выработки превентивных мер, адекватных ее изменениям. Для Республики Беларусь особое значение приобретает взаимодействие нашего государства по предотвращению преступлений в сфере высоких технологий с другими государствами в рамках СНГ. Отсутствие специального международного соглашения, устанавливающего правовые основы противодействия преступности в сфере высоких технологий, и наличие ряда существенных различий не только в материальном и процессуальном уголовном законодательстве государств – участников СНГ, но и в критериях, связанных с определением значимости угрозы указанного вида преступлений, не позволяют говорить об эффективности существующих механизмов международного сотрудничества в борьбе с преступлениями в сфере высоких технологий.

Современная преступность приобретает транснациональный характер, расширяя сферы своего влияния. Негативные последствия данного явления препятствуют формированию благоприятных условий для социально-экономического развития нашего общества, а также подрывают механизмы обеспечения безопасности и укрепления правопорядка в белорусском государстве.

УДК 343.7

К.А. Мартинович, следователь постоянно действующей группы по расследованию преступлений в сфере высоких технологий, Дрибинский районный отдел Следственного комитета Республики Беларусь
starlp9@mail.ru

ПРОБЛЕМНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ БАНКОВСКИХ ПЛАТЕЖНЫХ КАРТОЧЕК И ДЕНЕЖНЫХ СРЕДСТВ С НИХ

В последние годы кредитно-финансовые отношения как в Республике Беларусь, так и в других странах мира развиваются, являя нам все более новые и совершенные формы оплаты услуг, приобретения и покупки товаров, иных денежных операций. Одной из таких форм являются безналичные расчеты, осуществляемые с использованием банковских платежных карточек (БПК), активность обращения которых увеличивается каждый год. Общество постепенно переходит на ту ступень финансовых отношений, когда большая часть финансовых сбережений

хранится не в материальном виде, а именно на БПК. Издревле тяга к обогащению одолевала отдельными категориями граждан, не желающих самостоятельно зарабатывать на жизнь, ищущих легкие пути получения желаемого, и подталкивала к совершению хищений денежных средств, богатств, сокровищ и иных средств обогащения. С течением времени денежные средства и богатства в материальном виде стали замещаться банковскими платежными карточками. Соответственно, БПК все чаще стали являться непосредственным предметом преступления в уголовно-правовом значении.

В Республике Беларусь с ростом совершения преступлений, направленных на хищение БПК и с использованием БПК, правоприменительная практика пошла по пути квалификации таких хищений по ст. 212 Уголовного кодекса Республики Беларусь (УК). Эта норма уголовного законодательства предусматривает ответственность за хищение с использованием компьютерной техники.

За прошедшие годы написано немало научных трудов, рассматривающих вопросы квалификации хищений с использованием БПК. Некоторые авторы приводят доводы в поддержку сложившейся практики, другие ученые эти доводы оспаривают и считают данную правоприменительную практику в корне неверной. Однако, несмотря на все дискуссии в научном мире, обусловленные, как правило, различными подходами к трактовке как способов выражения объективной стороны состава преступления, предусмотренного ст. 212 УК, так и диспозиции этой статьи, исходя из анализа практики квалификации хищений денежных средств с использованием БПК, в подавляющем большинстве случаев рассматриваемые преступные деяния квалифицируются по ст. 212 УК. По нашему мнению, данный подход является абсолютно неверным, чему и будет дано дальнейшее обоснование.

Диспозиция ст. 212 УК содержит такие способы выражения объективной стороны, как изменение информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо введение в компьютерную систему ложной информации.

Для разбора диспозиции вышеуказанной статьи рассмотрим пример. К., воспользовавшись отсутствием внимания со стороны М., у которого он находился в гостях, с целью хищения денежных средств открыл кошелек М., откуда достал БПК, принадлежащую М., и листочек бумаги с записанным на нем ПИН-кодом, после чего, придя к ближайшему банкомату, вставил БПК в считывающее устройство для карточек, ввел ПИН-код, указанный на листочке бумаги, и обналичил денежную сумму в размере 300 р. Сопоставляя действия К. с объективной стороной ч. 1 ст. 212 УК, можно отметить следующее: К. никоим

образом своими действиями не изменяет информацию, обрабатываемую в компьютерной системе (банкомате), хранящуюся на машинных носителях (в данном случае машинным носителем выступает БПК) или передаваемую по сетям передачи данных, а также не вводит никакой ложной информации в компьютерную систему. Некоторые авторы считают, что ввод ПИН-кода от БПК, владельцем которой не является злоумышленник, и является вводом ложной информации, так как преступник выдает себя за владельца карточки, неправомерно пользуясь ею. Однако такой подход сложно назвать верным, так как К. вводит правильный ПИН-код, а иной информации, такой как, например, Ф.И.О. владельца карточки, кроме ПИН-кода, при снятии денежных средств с БПК не требуется. Возникает справедливый вопрос, для кого вводимая информация является ложной и в чем суть ее ложности?

В соответствии с абз. 1 п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищении имущества» хищение путем использования компьютерной техники возможно лишь посредством компьютерных манипуляций, которые заключаются в обмане потерпевшего или лица, которому имущество вверено или под охраной которого находится, с использованием системы обработки информации. Данное хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации.

С тем, что изменения информации, а также ввода ложной информации в действиях К. не усматривается, мы уже разобрались. Но также в компьютерных манипуляциях, проводимых К. (снятие денег с БПК с использованием банкомата), отсутствует и обман потерпевшего или лица, которому имущество вверено или под охраной которого находится. Снятие денег с использованием банкомата является автоматизированным процессом, и никакое физическое лицо, которое должно одобрить данную операцию, за этим процессом не стоит. Банкомат как автоматизированная система не может определить, правомерно или нет были сняты денежные средства с той или иной БПК. Таким образом, К., похитив БПК М., совершил приготовление к хищению денежных средств с БПК, а дальнейшие действия К., выразившиеся в хищении денежных средств с БПК с использованием банкомата, необходимо квалифицировать по ч. 1 ст. 205 УК как кражу, а оснований для применения ст. 212 УК нет.

Анализируя вышеизложенное, целесообразно окончательно изменить подход к квалификации хищения БПК и последующего хищения с

текущего (расчетного) банковского счета, к которому привязана БПК, денежных средств, в пользу ст. 205 УК, и издание соответствующих нормативных правовых актов, закрепляющих в себе данный подход. Альтернативным вариантом решения данной правоприменительной проблемы может послужить внесение изменений в текст ч. 1 ст. 212 УК, в котором будет отражаться помимо имеющихся способов выражения объективной стороны такой способ, как хищение имущества путем использования банковской платежной карточки.

Таким образом, закрепление на практике вышеуказанного правоприменительного подхода, либо изменение формулировки диспозиции уголовно-правовой нормы будет способствовать более эффективной борьбе с преступностью в кредитно-финансовой сфере.

УДК 343.9.01

Л.Л. Мельник, следователь по особо важным делам главного следственного управления центрального аппарата Следственного комитета Республики Беларусь
l_melnik@sk.gov.by

О КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ КРИПТОВАЛЮТЫ КАК ПРЕДМЕТА И ПЛАТЕЖНОГО СРЕДСТВА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

В настоящее время правоохранительные органы, в том числе Республики Беларусь, столкнулись с новыми разновидностями преступных посягательств, предметами и платежными средствами совершения которых выступает криптовалюта. После правового урегулирования понятия криптовалюты в белорусском законодательстве в 2017 г., придания ей статуса объекта гражданских прав, который охраняется, в том числе и уголовным законом, наблюдается рост числа зарегистрированных преступлений с ее использованием. В течение 2018 г. возбуждено 6 уголовных дел, а за 10 месяцев 2019 г. – 13 уголовных дел, предметом преступления которых явилась криптовалюта, при этом из вышеуказанных 19 уголовных дел только по одному установлено лицо, совершившее хищение криптовалюты (ст. 212 Уголовного кодекса Республики Беларусь (УК)), остальные в настоящее время являются нераскрытыми. Наряду с вышеназванными уголовными делами в производстве следователей находятся уголовные дела, по которым криптовалюта выступает платежным средством совершения преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, распространением порнографических материалов, в том числе с изображением несовершеннолетних. Можно полагать, что в последующие годы количество преступлений, в процессе совершения которых предметом и платежным средством выступит криптовалюта, будет увеличиваться.

В связи с цифровизацией жизнедеятельности общества, увеличением разнообразия способов хранения и накопления капиталов посредством криптовалют, в том числе представителями теневого рынка и преступной среды, назрела необходимость разработки методики расследования преступлений данной направленности. Ключевым блоком данной методики является криминалистическая характеристика преступления, в структуре которой характеризующая криминалистически значимая информация о криптовалютах выступает в качестве одного из основных элементов.

Криптовалюта как предмет преступного посягательства имеет присущие только ей отличительные признаки, которые обусловлены использованием технологии блокчейн при функционировании (на примере наиболее распространенной криптовалюты Bitcoin). Описание признаков криптовалюты имеет важное криминалистическое значение, так как предполагает специфический порядок обнаружения, фиксации и осмотра, а также последующего анализа имеющейся информации («электронных следов»), влияет на установление фактов, в том числе использования криптовалют конкретными пользователями и их деанонимизации.

По нашему мнению, к криминалистически значимым признакам криптовалюты можно отнести:

нематериальную природу криптовалюты. Данный признак означает, что криптовалюта – неовеществленный предмет и существует в электронном виде, при этом относится в соответствии с белорусским законодательством к иному имуществу;

отсутствие единого эмиссионного центра в виде банковской системы или правительства, которые осуществляли бы выпуск и регулирование криптовалют;

использование в международном обороте согласно Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» (далее – Декрет);

криптовалюта – универсальное средство обмена (согласно Декрету);

анонимность использования криптовалюты;

необратимость проведения транзакций;

прозрачность проведения транзакций в блокчейне.

Полагаем, при характеристике криптовалюты криминалистическое значение имеют также следующие сведения:

о системе эмиссии (децентрализованная или централизованная);

системе осуществления транзакций (открытые или анонимные);

средствах регистрации и учета в системах криптовалют и криптобирж (предусмотрена ли возможность хранения о регистрационных данных, транзакциях и IP-адресах пользователей или нет);

правовой и организационной структуре систем криптовалют и криптобирж (юридическое лицо, его филиалы, их расположение и расположение серверов);

порядке осуществления обмена, взимания комиссии, средств учета в системах криптовалют и криптобирж;

порядке регистрации и использования криптокошельков;

блокчейн-обозревателях, позволяющих получить доступ к сведениям о проведенных транзакциях той или иной криптовалюты;

признаках микширования транзакций.

Приведенные признаки и характеристики криптовалют позволяют установить, является ли цифровой знак (токен) криптовалютой, а также получить и зафиксировать криминалистически важную информацию для расследования.

В настоящее время УК прямо не предусмотрены составы преступлений, где бы в качестве исключительного предмета или средства совершения преступления выступала криптовалюта. Среди преступлений, предусмотренных главами УК, следует выделить те, где криптовалюта может рассматриваться как предмет и платежное средство преступлений:

против собственности (вымогательство, мошенничество, хищение с использованием компьютерной техники);

против порядка осуществления экономической деятельности (легализация («отмывание») средств, полученных преступным путем; приобретение либо сбыт материальных ценностей, заведомо добытых преступным путем);

против информационной безопасности (несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией);

против интересов службы (получение взятки, дача взятки).

Таким образом, полученная криминалистическая характеристика криптовалюты открывает перспективы разработки криминалистической характеристики рассматриваемых преступлений и, соответственно, методик расследования преступных деяний, предметом или платежным средством совершения которых является криптовалюта.

УДК 343.9

Е.В. Михайлова, кандидат юридических наук, преподаватель кафедры криминологии Московского университета МВД России им. В.Я. Кикотя
kis-01@mail.ru

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМЫХ НЕСОВЕРШЕННОЛЕТНИМИ: ЗАРУБЕЖНЫЙ ОПЫТ

Современные информационные технологии – неотъемлемая часть всех сфер жизнедеятельности личности, общества и государства. Однако, наряду с положительными достижениями, сфера компьютерных технологий повлекла за собой негативные последствия, в том числе увеличение количества преступлений с использованием информационно-телекоммуникационной сети Интернет, позволяющей безнаказанно совершать традиционные преступления (кража, мошенничество, вымогательство), а также неизвестные ранее мировому сообществу виды общественно опасных посягательств (неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ).

Количество пользователей сетью Интернет во всем мире стремительно увеличивается, что определяет постоянный рост размера причиняемого ущерба. По объему потенциального ущерба аналитики Всемирного экономического форума ставят киберпреступность на седьмое место в списке основных глобальных рисков: она опережает техногенные экологические катастрофы и распространение инфекционных заболеваний.

Эксперты международной консалтинговой фирмы Accenture утверждают, что в 2018 г. кибератаки в среднем обошлись одной компании в 13 млн долл., что на 12 % дороже, чем в 2017 г., в 2018 г. общие потери мировой экономики из-за действий хакеров составили 1,5 трлн долл., а в 2019 г. эта сумма выросла до 2,5 трлн долл. В соответствии с ежегодным отчетом «Hi-Tech Crime Trends 2018» каждый месяц в России успешно атакуют 1-2 банка, средний ущерб от кибератаки – 132 млн р., ущерб экономике Российской Федерации в 2018 г. составил свыше 1,1 трлн р.

И если за организацией целевых атак на банки или иные организации, как правило, стоят опытные люди, обладающие специальными знаниями, то противоправные действия в отношении физических лиц

совершают лица, не обладающие особыми знаниями в сфере компьютерных технологий, в том числе подростки. В соответствии с результатами исследования кибербезопасности «Threat Zone 17/18: новые вызовы цифрового мира», от 30 % до 40 % киберпреступлений совершаются подростками в возрасте от 14 до 16 лет.

По словам экспертов по кибербезопасности, малолетние хакеры в настоящее время представляют реальную угрозу. «Многие преступные сообщества сегодня занимаются тем, что рекрутируют таких интернет-умельцев в свои ряды. Сейчас почти каждый ребенок вырастает с компьютером в руках. И технологии, которые они осваивают, далеко не всегда мирного назначения. Как правило, все начинается с каких-то шалостей – «на спор», ради хулиганства или самоутверждения. Однако потом это перерастает в нечто более серьезное. В дальнейшем они ломают сайты корпораций или потрошат банкоматы».

Действительно, если для школьников 14–15 лет характерно совершение преступных деяний из любопытства, желания испытать острые ощущения, приобщиться к виртуальному обществу, субкультуре, то подростки старшего возраста (16–17 лет) ищут возможности заработка, в том числе путем противоправных действий (переводы денег с чужого виртуального кошелька, взломы аккаунтов в соцсетях с целью шантажа, мошеннические схемы, создание вредоносного программного обеспечения «на заказ»).

Субъективно дети и подростки часто невероятно далеки от осознания последствий своей «сетевой жизни» и тем более от понимания правовых последствий взаимодействия с интернет-ресурсами. Их любознательность и оперативность впитывания информации на фоне отсутствия необходимого социального опыта и активных попыток переноса игровых сценариев в реальную жизнь постоянно питают почву для различных правонарушений.

Чтобы предупредить возможные риски, многие государства готовят специалистов по кибербезопасности со школьной скамьи. Так, в израильских школах с четвертого класса дети изучают программирование. Учеников, успевающих по этой дисциплине, рекомендуют к дополнительным занятиям по криптографии и кибербезопасности в сертифицированных центрах. В Великобритании проводятся ежегодные молодежные соревнования по кибербезопасности (с целью привлечения детей в 2015 г. одним из этапов соревнований стал специально разработанный уровень компьютерной игры Minecraft). Австралийское правительство с 2018 г. включило обязательное преподавание блокчейн (blockchain) и криптоалгоритмов в образовательную программу, начиная с младших классов, что позволяет дать детям финансовое и цифровое образование, а также значительно уменьшить цифровой разрыв

между детьми и взрослыми. Агентство национальной безопасности Америки открывает летние лагеря для студентов, школьников и даже воспитанников детских садов. Активно используется практика по созданию так называемых отрядов «белых хакеров» (white hacker), в которые входят школьники, хорошо владеющие информационными технологиями. Такие отряды успешно тестируют программное обеспечение на различные уязвимости. Для совершенствования навыков специалистов по информационной безопасности организуются командные соревнования CTF (Capture the flag) по информационной безопасности и системному администрированию. Крупнейшими международными соревнованиями считаются проводимые Калифорнийским университетом в Санта-Барбаре, победителем которых в 2018 г. стала команда студентов Томского государственного университета SiBears.

В 2008 г. в Республике Корея создана Международная федерация киберспорта, который в настоящее время прибрел огромную популярность во многих странах мира. По компьютерному спорту проводятся соревнования как для профессиональных спортсменов, так и для любителей, в том числе студентов и школьников. Кроме того, многие учебные заведения реализуют образовательные программы по компьютерным наукам в области игровых технологий. Так, профессиональный колледж Финляндии (Оривеси) Ahlman организует обучение по трем направлениям: «Технологии разработки компьютерных игр», «Дизайн компьютерных игр», «Киберспорт». В Республике Беларусь (Минск) открыта школа киберспортивного обучения Cyber Gaming School, а также летний лагерь для детей и подростков.

Активно развивается киберспорт и в Российской Федерации. С 2006 г. проводятся официальные соревнования для студентов, обучающихся в образовательных учреждениях высшего образования страны, а после официального признания компьютерного спорта в 2016 г. была организована Всероссийская киберспортивная студенческая лига (ВКСЛ).

Инициаторами образовательных проектов для школьников выступают коммерческие и некоммерческие организации, такие как Group-IB (образовательные программы по информационной безопасности), Акционерная финансовая корпорация «Система» («Лифт в будущее»), Samsung («IT-школа Samsung»). Программы, направленные на повышение цифровой грамотности детей, запускают и разработчики компьютерных игр (например, игра-стимулятор по изучению принципов работы искусственного интеллекта «while True: learn()» от российской студии Luden).

Однако в силу ряда причин (высокая стоимость, отсутствие образовательного центра в регионе проживания, недостаточный уровень базовых знаний) такие проекты недоступны для широкой аудитории школьников.

В целях предупреждения совершения компьютерных преступлений целесообразно заниматься правовым, информационным воспитанием детей путем внедрения в школы программ повышения компьютерной грамотности, стандартов этических норм поведения в цифровой среде, соблюдения прав других граждан, ограничений, установленных законодательством, стимулировать интерес родителей к анализу медиапродукции, предпочитаемой их детьми, осуществлять контроль за интернет-сайтами, посещаемыми ребенком, стать активными участниками в процессе воспитания норм поведения в цифровом мире.

УДК 351.745.7

А.В. Мовчан, доктор юридических наук, профессор, профессор кафедры оперативно-розыскной деятельности Львовского государственного университета внутренних дел (Украина)
movchan.anatol@gmail.com

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ ПОДРАЗДЕЛЕНИЯМИ КИБЕРПОЛИЦИИ НАЦИОНАЛЬНОЙ ПОЛИЦИИ УКРАИНЫ

Термин «компьютерная преступность» (computer crime) часто употребляется наряду с термином «киберпреступность» (cybercrime), причем нередко эти понятия используются как синонимы. Согласно Закону Украины «Об основных принципах обеспечения кибербезопасности Украины» киберпреступление (компьютерное преступление) – общественно опасное виновное деяние в киберпространстве и/или с его использованием, ответственность за которое предусмотрена Законом Украины «Об уголовной ответственности» и/или которое признано преступлением международными договорами Украины.

В разд. XVI Уголовного кодекса (УК) Украины «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи» закреплены ст. 361, 361-1, 361-2, 362, 363, 363-1, которые устанавливают ответственность за такие деяния.

Согласно данным официальной статистики, в Украине за 9 месяцев 2019 г. зарегистрировано 1 796 уголовных правонарушений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей или сетей электросвязи, в том числе:

несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи (ст. 361 УК Украины) – 1 014;

несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней (ст. 362 УК Украины) – 576;

создание с целью использования, распространения или сбыта вредоносных программных или технических средств, а также их распространение или сбыт (ст. 361-1 УК Украины) – 165;

несанкционированные сбыт или распространение информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361-2 УК Украины) – 33.

Одним из субъектов противодействия компьютерной преступности в Украине являются подразделения киберполиции Национальной полиции. В частности, основная задача Департамента киберполиции Национальной полиции Украины – участие в формировании и обеспечении реализации государственной политики по предупреждению и противодействию уголовным правонарушениям, механизм подготовки, совершения или сокрытия которых предусматривает использование электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи.

Например, в сентябре 2019 г. полицейские Департамента киберполиции Национальной полиции Украины разоблачили хакера, который за время своей преступной деятельности получил несанкционированный доступ к тысячам серверов пострадавших из более чем 100 стран мира. Полученные инструменты он использовал как для продажи данных, так и для получения доступа к банковским аккаунтам и платежным системам.

Для привлечения клиентов 29-летний житель Харькова размещал на специализированных сайтах и форумах объявления о продаже доступов к удаленным серверам. Для оплаты таких услуг использовались электронные платежные системы.

Полицейские провели несколько обысков по адресам, где проживал хакер, в результате которых были изъяты компьютерная техника, деньги и внешние носители информации. Во время предварительного осмотра техники киберполиция обнаружила активные сессии и перечень взломанных серверов с учетными данными доступа к ним. По данному факту проводится досудебное расследование, квалифицированное по ч. 2 ст. 361 УК Украины.

Полицейские киберполиции также разоблачили преступную группу из пяти человек во главе с 34-летним организатором, которые в течение последних двух лет создавали и продавали в сети вредоносные технические средства, предназначенные для несанкционированного вмешательства в работу систем снабжения и учета потребленной электроэнергии. В дальнейшем эти аппаратные комплексы настраивались и использовались для блокирования работы процессора электросчетчика, в результате чего энергоснабжающие предприятия несли миллионные убытки.

Для сбыта этих устройств организатор преступной группы создал отдельный интернет-сайт. В зависимости от вида электросчетчика стоимость каждого такого технического средства колебалась от 3 до 15 тыс. гривен. Таким образом злоумышленники заработали более миллиона гривен.

Полицейские изъяли во время обыска изготовленные технические средства и оборудование для их изготовления, компьютерную технику, дополнительные носители информации, банковские платежные карточки, деньги и мобильные телефоны. По данному факту проводится досудебное расследование в рамках начатого производства по ст. 361, 361-1 УК Украины.

11 сентября 2019 г. в ходе проведения в Киеве форума «Cellebrite User Forum Kyiv 2019» специалисты компании Cellebrite и Лаборатории компьютерной криминалистики «ЕПОС» рассказали участникам конференции о своих наработках в течение последнего года и поделились лучшими практиками последних достижений цифровой криминалистики.

Как отметил на форуме руководитель Департамента киберполиции Национальной полиции Украины С. Демедюк, бороться с компьютерной преступностью государству самостоятельно трудно. Ведь технологии развиваются поминутно, а преступники постоянно совершенствуют свои схемы, чтобы максимально скрыть следы.

Сегодня преступники перестают пользоваться аналоговыми каналами связи и классическими местами для хранения информации. Все чаще они используют облачные сервисы хранения информации и абузостойкие хостинги, которые не контролируются со стороны государства.

Для киберполиции важно использовать современные высокотехнологичные инструменты для получения доказательной базы. Благодаря сотрудничеству с частными организациями полицейским киберполиции удается получать данные, которые в дальнейшем используются в качестве цифровых доказательств.

Кроме того, с помощью качественной аналитики Национальная полиция получает не только доказательства противоправной деятельности, но и выявляет новые преступления.

Для того чтобы уберечь свои данные от постороннего вмешательства, киберполиция рекомендует пользователям компьютеров:

устанавливать актуальные обновления операционной системы;

использовать исключительно лицензионное программное обеспечение;

использовать современные антивирусные программы и постоянно обновлять их;

использовать только надежные пароли (состоящие из букв, чисел и символов).

УДК 339.13

А.В. Осипов, магистр, аспирант Академии управления при Президенте Республики Беларусь
7744222@tut.by

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЦЕЛЯХ ПОВЫШЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Блокчейн – база данных, безопасность которой обеспечивается механикой распределенного консенсуса. Первой широко принятой реализацией блокчейна является биткоин, для которого база данных – просто временная книги платежей. Первоначально разработанная как технология, лежащая в основе цифровой валюты биткоин, она вскоре стала распространяться за пределы криптовалют. Некоторые ученые называют систему блокчейн «машиной доверия». Из-за использования различных криптографических методов и их децентрализованного и распределенного характера, блокчейны, по заявлению экспертов, очень устойчивы. Прозрачный, безопасный и неизменный характер блокчейна вызвал интерес как частного сектора, так и государственных органов. Количество доказательств прозрачности работы технологии «блокчейн» и пилотные проекты в данном секторе стремительно растут во всем мире, а технология уже стала применяться во всех секторах экономики и общества – от финансов до электронной торговли, продовольственной безопасности, управления и даже голосования.

Проблемы экономической безопасности и трудности координации информационных и финансовых потоков через границы и между несколькими странами, участвующими в международной торговле, затруднят усилия по цифровизации работы системы государственных закупок. Новую технологию, блокчейн, многие видят как возможный

гейм-чейнджер. В новом документе, подготовленном экспертами, связанными с группой Всемирного банка, предлагается создать блокчейн-сеть для повышения эффективности систем государственных закупок по всему миру.

Общепринятым термином, который описывает этот класс технологий, являются «умные контракты», которые характеризуют новую модель построения бизнес-контрактов, в которых определение, выполнение и проверка непредвиденных обстоятельств происходят как выполнение кода на блокчейне, а не как обязанности доверенной третьей стороны. Данные, введенные в блокчейн, «хэшируются», т. е. преобразуются в новый цифровой формат (строка фиксированной длины с использованием математической функции и зашифрованная для обеспечения целостности данных, предотвращения подделки и гарантии того, что сообщение было создано и отправлено заявленным отправителем и не было изменено в пути). Если отправитель транзакции не желает, чтобы другие участники сети видели содержимое самого сообщения (т. е. данные открытого текста, содержащиеся в представленных документах), он/она может выбрать шифрование самого сообщения, тем самым делая данные непонятными для лиц без разрешенного доступа.

Перспектива проецирования сложных бизнес-процессов на код и устранения дорогостоящих посредников уже капитализировала более 1 млрд долл. венчурных инвестиций в данную технологию за 2018 г. Этот преобразующий потенциал блокчейна может также революционизировать, а его ключевые функции могут быть успешно применимы в государственном секторе.

Марк Уолпорт, главный научный советник правительства Великобритании, недавно опубликовал доклад, в котором изучаются потенциальные преимущества использования технологии блокчейн в государственном секторе. Блокчейн, по мнению ученого, создает волны в коммерческом секторе – особенно в сфере финансовых услуг – и может считаться одним из самых значительных достижений в области технологий нового поколения. Данная технология идеально подходит там, где есть необходимость в защищенном от несанкционированного доступа центральном учете. Обмен информацией имеет решающее значение для многих бизнес-процессов, которые лежат в основе государственных услуг. Конечно, жизненно важно, чтобы эти данные хранились надежно, и блокчейн чрезвычайно трудно взломать из-за его концепции работы.

Поскольку государственный сектор стремится создать более эффективные способы предоставления услуг для своих граждан, блокчейн может стать ключевой базовой технологией в этой сфере. В докладе М. Уолпорта также рекомендуется правительству использовать блок-

чейн для повышения подотчетности на местном уровне и снижения зависимости от централизованного правительства, что связано с растущей потребностью в сотрудничестве между государственными служащими и различными ведомствами. Блокчейн может уменьшить мошенничество, ошибки, а также время и стоимость бумажно-интенсивных процессов, делая государственный сектор более прозрачным для своих граждан.

Для Республики Беларусь система блокчейн открывает множество возможностей не только для государственных структур. На сегодня статус криптовалют не имеет устойчивой законодательной базы, но уже выносят на рассмотрение первые нормативные правовые акты. Существуют стартовые проекты с использованием технологии блокчейн, которые частично реализованы на государственном уровне. Технологию блокчейн будут использовать в самых разных сферах общественной деятельности. Для Республики Беларусь очень перспективной возможностью является использование блокчейн для электронного голосования, что улучшит уровень демократии. Существует множество возможностей использования и внедрения технологии для электронного денежного обращения, документооборота и др. Такая технология имеет свои положительные и отрицательные стороны, поэтому надо учитывать возможные угрозы и слабые стороны системы.

Следует выделить ключевые особенности блокчейна в системе государственных закупок:

1) *Децентрализованная, распределенная и прозрачная архитектура.* Информация, добавленная в блокчейн, сразу видна всем участникам сети Интернет и распределена, т. е. каждый узел сохраняет полную копию данных (или как можно ближе к ней) и обновления, если таковые имеются, совместно используются всей сетью без необходимости доверять одному третьему лицу.

2) *Высокий уровень безопасности, неизменяемость и прослеживаемость.* Одновременное использование различных криптографических методов децентрализованного и распределенного методов блокчейн-платформ делает их высокоустойчивыми к атакам по сравнению с традиционными базами данных. Однако, хотя сама технология обеспечивает высокий уровень безопасности, слабые места остаются в отношении умных контрактов и закрытых ключей, используемых для шифрования, которое может быть украдено с помощью обычных атак, если они будут сохранены на компьютере отдельного пользователя или на централизованном сервере.

Независимо от этого существуют также значительные ограничения для технологии блокчейн в государственном секторе, и их не следует рассматривать как полностью комплексное решение само по себе.

Фундаментальные проблемы, не решаемые непосредственно блокчейном, двояки. Во-первых, технология блокчейн оптимизирована для поиска плохих транзакций, а не плохих акторов. Во-вторых, блокчейн обеспечивает только экономичное и безопасное пространство данных для измерений. Для того чтобы анализ на таком пространстве данных был полезен, все еще должна быть критическая плотность и объем высококачественных измерений событий в цепочке. В то время как технология блокчейн обеспечит экономичное, безопасное и единообразное пространство данных для записи таких событий, специальная экспертиза, включенная блокчейном, идеально подходит для выявления злого умысла в деловых отношениях на уровне исполнения государственных контрактов. Однако у отдельного «недобросовестного» субъекта внутри предприятия (организации исполнителя/поставщика), скорее всего будет множество способов избежать обнаружения, если он знает о пробелах в процедурах безопасности в своей организации и вокруг нее, таких как диапазон событий реального пространства, не учитываемых блокчейном.

Таким образом, технология блокчейн не будет полностью заменять надежные процедуры проверки персонала и мониторинга его деятельности. Кроме того, для того чтобы даже аналитика на уровне предприятия или государства была эффективной, физические пространства и электронные процессы, влияющие на выполнение государственных контрактов, должны быть снабжены приборами с плотностью и распределением датчиков, соизмеримыми с тонкостью искомых явлений. Разработка и развертывание данных датчиков в таком масштабе является нетривиальной проблемой сама по себе. Ожидается, что любое широко эффективное решение проблемы безопасности в системе государственных закупок потребует сочетания подходов, из которых блокчейн будет одной из многих частей.

Открытость и прозрачность работы всей системы государственных закупок Республики Беларусь – реальность, с которой политикам придется бороться в условиях все более открытой глобальной экономики. Технология блокчейн сама по себе не обеспечит полного решения проблемы. В целом решения на основе блокчейна являются лишь одним инструментом из широкого спектра инструментов, необходимых для обеспечения безопасности государственных контрактов, предоставляя инструменты для специализированной экспертизы для обнаружения противоправных действий. Полная трансформация работы системы государственных закупок Республики Беларусь для размещения блокчейна может потребовать долгосрочных, общегосударственных и общепромышленных усилий, но может быть экспериментально реализована в краткосрочной перспективе в небольших масштабах. В таких экспериментах можно начать разрабатывать данные, необходимые для решения более широких вопросов возврата инвестиций блокчейн-подходов, по сравнению с подходами, основанными на традиционном экономическом анализе.

Обеспечение безопасности и прозрачности работы государственных органов в системе государственных закупок посредством применения технологии блокчейн – системная инженерная задача беспрецедентных размеров. По существу проблема заключается в том, чтобы контролировать совокупность коммерческой деятельности, которая связана с добросовестным исполнением государственных контрактов. Блокчейн как новая технология влечет за собой экстраординарные риски, он также несет экстраординарные перспективы как инструмент, уникально подходящий для проблем особого масштаба и сложности.

УДК 343.98

И.В. Пашута, кандидат юридических наук,
доцент, доцент кафедры криминалистики
Академии МВД Республики Беларусь
pashutaiv@yandex.ru

ОЦЕНКА ЗАКЛЮЧЕНИЯ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Раскрытие и расследование преступлений против информационной безопасности, а также совершенных с использованием компьютерной техники, трудно представить без назначения судебной компьютерно-технической экспертизы, оценка которой и по сей день вызывает сложности у практических работников органов, ведущих уголовный процесс.

Фактические данные, содержащиеся в заключении эксперта, как один из видов доказательств, оцениваются органом уголовного преследования и судом, по общим правилам оценки доказательств (ст. 105 Уголовно-процессуального кодекса Республики Беларусь (УПК)). При этом особенностью заключения эксперта, как источника доказательств, является то, что оно содержит выводы по поставленным перед экспертом вопросам, основанным на специальных знаниях эксперта в области науки, техники, искусства, ремесла и иных сферах деятельности, которыми не располагают следователь, лицо, производящее дознание, прокурор, суд.

Процесс оценки экспертного заключения по проведенной судебной компьютерно-технической экспертизе предлагается осуществлять по следующим этапам:

1. Определение относимости (определение связи полученного доказательства с предметом доказывания либо его отдельными элементами). Относящимися к уголовному делу признаются фактические данные, содержащиеся в заключении эксперта по проведенной судебной компьютерно-технической экспертизе, посредством которых устанавливаются обстоятельства, имеющие значение для уголовного дела (диагностирование программного продукта как вирусного, установление факта изменения первоначального состояния программы, установление причинной связи между действиями пользователя компьютерной системы в отношении программного обеспечения и наступившими последствиями и др.);

2. Определение допустимости (заключается прежде всего в установлении соблюдения требований УПК при назначении и проведении экспертизы). Проверка соблюдения требований закона при назначении и проведении судебной компьютерно-технической экспертизы состоит в установлении следующих вопросов: произведена ли экспертиза правомочным субъектом (специалистами экспертных учреждений, иных государственных или негосударственных организаций, назначенными органом, ведущим уголовный процесс); не заинтересован ли эксперт в исходе уголовного дела и отсутствуют ли основания для его отвода (ст. 85 УПК); компетентен ли эксперт в решении поставленных ему задач и не вышел ли он за пределы своей компетенции; соблюден ли порядок назначения экспертизы (имеется ли подписка эксперта о разъяснении ему прав и обязанностей, предупреждении об ответственности и др.); соблюдены ли требования получения и обеспечения сохранности (упаковка и условия хранения) объектов экспертного исследования; надлежащим ли образом произведено процессуальное оформление хода и результатов экспертного исследования;

3. Определение достоверности (определение соответствия данных, полученных при производстве судебной компьютерно-технической экспертизы, действительности, их научная обоснованность). При оценке содержательной стороны заключения эксперта анализируются: научная обоснованность примененной экспертом методики; полнота, объективность и всесторонность проведенного исследования; логическая обоснованность хода и результатов исследования, аргументированность выводов.

Научная обоснованность примененной экспертом методики (методика изучения программных средств, методика исследования компьютерной информации, методика непосредственного изучения аппаратных средств) является наиболее сложным компонентом оценки заключения эксперта для лиц, не обладающих специальными знаниями. Опорой для субъекта исследования доказательств здесь может служить различная справочная и научно-методическая литература. По мнению Е.П. Ореховой, можно также учитывать ряд формальных критериев: включена ли методика в Реестр методик Государственного комитета судебных экспертиз Республики Беларусь, рекомендована ли методика к использованию в судебно-экспертной деятельности, и т. п.

При определении полноты, объективности и всесторонности проведенного исследования устанавливается следующее: правильно ли применен тот или иной метод (совокупность методов) исследования (методы проектирования и исследования цифровых устройств и микропроцессоров, методы восстановления данных, архивации, парольной защиты и др.); исследованы ли все представленные на экспертизу объекты и материалы; даны ли аргументированные ответы на все поставленные перед экспертом вопросы; полно и всесторонне ли описан ход и результаты исследования и приложен соответствующий иллюстративный материал.

Неполнота экспертного исследования и оформления его заключения является основанием для назначения дополнительной либо повторной экспертизы, а также допроса эксперта.

Логическая обоснованность хода и результатов исследования, аргументированность выводов производится путем анализа последовательности стадий экспертного исследования, соответствие выводов эксперта промежуточным исследованиям и всему исследованию в целом, их непротиворечивость и т. д. (вывод может не являться логическим следствием проведенного экспертного исследования, быть недостаточно мотивированным; по одному и тому же объекту (предмету) могут быть даны противоречивые выводы экспертов);

4. Определение достаточности. Сопоставление имеющихся в заключении судебной компьютерно-технической экспертизы выводов с другими доказательствами может образовывать совокупность, позволяющую установить те или иные обстоятельства, подлежащие доказыванию по уголовному делу;

Предложенный алгоритм, как видится, позволит более эффективно проводить оценку заключения эксперта по судебной компьютерно-технической экспертизе при раскрытии и расследовании преступлений против информационной безопасности, а также совершенных с использованием компьютерной техники.

УДК 343.3/7

А.К. Раев, магистр юридических наук, старший преподаватель-методист, майор полиции Алматинской академии МВД Республики Казахстан им. М. Есбулатова
mvdas88@gmail.com

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ КАЗАХСТАН

Основной причиной возникновения компьютерной преступности априори можно назвать возникновение и быстрое развитие самих информационных технологий. Иначе говоря, до XX в. компьютерные преступления не регистрировались именно в силу объективной невозможности их совершения, отсутствия компьютеров и компьютерных технологий.

Современное развитие кибериндустрии способствует созданию самых различных инструментов, используемых для совершения компьютерных преступлений. При этом все компьютерные преступления, на наш взгляд, можно разделить на две основные группы.

Первая группа охватывает преступные деяния, совершаемые с помощью современных технологий, позволяющих посредством информационно-коммуникационных сетей совершить любое преступное деяние, не исключая даже убийство. Так, широкую известность получил случай из практики США, где раненый при покушении свидетель, находящийся под программой государственной защиты, был помещен в охраняемую палату в больнице. Преступники смогли довести до конца свой замысел на убийство свидетеля путем изменения компьютерной программы прибора стимуляции сердца, незаконно подключившись к сети Интернет больницы. Еще большее распространение получили преступления против собственности (кражи со счетов, интернет-мошенничества и др.), совершаемые с применением компьютеров. Такие деяния отличаются от классических преступлений лишь использованием компьютерных технологий в качестве орудий совершения преступления.

Вторая группа компьютерных преступлений – преступные деяния, совершаемые непосредственно внутри информационно-коммуникационной сферы (действия хакеров, взломщиков, Doc-злоумышленников и др.). Эти компьютерные преступления непосредственно посягают на безопасность информационных сетей.

Следует отметить, что в Уголовном кодексе Республики Казахстан (УК РК) 2014 г. предусмотрена специальная гл. 7 «Уголовные правонарушения в сфере информатизации и связи», в которую включены составы преступлений, непосредственно связанных с информационными правоотношениями, т. е. деятельностью с информацией как самостоятельным объектом.

Развитие информационных сетей и само создание глобальной компьютерной сети Интернет во многом расширило обычные границы представлений и деятельности человека, при этом реалии менялись столь стремительно, что сфера законодательства не успевала их охватить – это появление принципиально новых технологий, новых угроз безопасности, новых видов и новых способов и средств совершения преступных деяний.

Необходимо осознавать при этом всю сложность проблем, с которыми пришлось столкнуться отечественным законодателям при формировании такой новой подотрасли права, как информационное право. Прежде всего это отсутствие единого подхода в выборе и использовании терминов в данной сфере. Мнения теоретиков достаточно сильно различаются даже по поводу самого понятия «информация» в праве.

Терминологическая неопределенность повлекла за собой неопределенность в определении объектов информационных отношений как объектов правовой охраны. Кроме того, сложность рассматриваемой сферы правоотношений требует от законодателя и правоприменителей достаточно высокой квалификации и наличия определенного уровня знаний в области информационно-технической деятельности.

Исходя из вышеизложенного можно говорить о возникновении относительно обособленной группы общественных отношений – информационных отношений, выделяемых по признаку информации как объекта этих отношений. Действия субъектов права, связанные с созданием, передачей, обменом, хранением, потреблением, распространением и иным оборотом информации, информационных ресурсов, – основные объекты правового регулирования, которые могут и должны быть урегулированы правом. Следовательно, можно вести речь о формировании новой комплексной отрасли права – информационного права.

Вопрос о существовании данной отрасли сам по себе является спорным. В Российской Федерации такая отрасль включена в номенклатуру специальностей научных работников. В Республике Беларусь информационное право также признано самостоятельной отраслью науки, по которой присуждаются ученые степени (12.00.13). В Казахстане в правовых специальностях такого направления пока не предусмотрено.

Полагаем, что выделение информационного права как самостоятельной отрасли правовой науки полностью обоснованно. Прежде всего это подтверждается наличием информационных отношений как самостоя-

тельного предмета правового регулирования. Информационные правоотношения связаны с компьютерными процессами сбора, создания, обработки, распространения информации, направленными на решение информационных запросов граждан, организаций, общества и государства. Учитывая, что разнообразие существующих информационных отношений актуализирует вопрос об обеспечении информационной безопасности, правовое регулирование этих отношений, определение возможных деликтов и установление мер юридической ответственности за их совершение представляется логичным и необходимым шагом.

Важный момент заключается в том, что сегодня от уровня эффективности использования информации зависит общий уровень развития государства, обеспечения безопасности общества и граждан. Охраняемая нормами уголовного права информация – лишь небольшая часть всех информационных ресурсов. Постоянное увеличение как количества, так и видов преступлений в сфере информации диктует необходимость уточнения объективной стороны составов соответствующих уголовных правонарушений, а также дифференциации уголовной ответственности виновных лиц. Полагаем, не подлежит сомнению неизбежность будущих изменений уголовного закона в части информационных уголовных правонарушений.

УДК 004:343

Н.И. Рудович, кандидат юридических наук, доцент учреждения образования «Белорусский государственный экономический университет»
Roodnik@mail.ru;
Е.О. Ковалёва, студентка учреждения образования «Белорусский государственный экономический университет»
Katia.10.12.2000@gmail.com

СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ПОРЯДКА ПРОВЕДЕНИЯ ЭЛЕКТРОННЫХ РАСЧЕТОВ

Система «Home Banking» получила широкое распространение в 80-х гг. прошлого столетия в США. Основная задача данной системы – обеспечение технической возможности клиентам банка контролировать свои счета. С развитием информационных технологий и расширением спектра оказываемых услуг банками своим клиентам была предложена дополнительная функция перевода денежных средств. Благодаря своей многофункциональности и удобству использования, система «Home Banking» приобрела широкое распространение за пределами США.

В странах постсоветского пространства данная система стала использоваться в гражданском обороте в конце 1990-х гг. Несмотря на некоторые трудности ее внедрения в банковском секторе, можно говорить о том, что сегодня онлайн-банкинг имеет повсеместное использование в различных сферах деятельности граждан указанных государств.

Доступность и удобство использования онлайн-банкинга в современных условиях привлекает множество клиентов, и, вполне очевидно, что в вопросах онлайн-расчетов на первое место выходит их безопасность. Интернет-банкинг предоставляет возможность беспроблемного доступа к использованию банковской платежной карточки: чтобы провести операцию необходимо иметь доступ в онлайн-банк и соответствующие пароли. Следовательно, основной задачей участников расчетных отношений в таких случаях становится обеспечение безопасности личного кабинета.

Актуальность обеспечения безопасности данной формы расчетов обусловлена частыми случаями несанкционированного доступа к средствам клиентов на счетах. Специалисты в сфере противодействия преступлениям, совершенным с использованием высоких технологий, выделяют несколько основных причин угрозы безопасности. Так, текущей основной проблемой безопасности данных в Интернет-банкинге является фишинг. Злоумышленники, представляясь официальной организацией, рассылают ложные сообщения клиентам с просьбой сообщить личные данные. Телефонный «фишинг» работает аналогично обычному, только в этом случае клиенту поступают звонки от лжепредставителей банка. Возможно также похищение баз данных в самом банке. В таком случае злоумышленник может получить доступ к множеству счетов клиентов. Как правило, в подобных случаях убытки полностью возмещаются самим банком, не дожидаясь поимки мошенников. Достаточно распространенная схема получения паролей и логинов путем внедрения различных вирусных программ, которые могут устанавливаться как на компьютеры, так и на телефоны или планшеты.

Широкое распространение в электронных расчетах параллельно компьютерному онлайн-банкингу получили мобильные приложения для смартфонов и планшетов. Они достаточно эффективны и удобны в использовании, а по функционалу мало отличаются от компьютерного онлайн-банка. Однако, как отмечают специалисты, в случае входа в Интернет-банк через мобильное устройство риск взлома персональных данных в разы увеличивается.

Среди основных методов защиты данных от противоправного проникновения со стороны третьих лиц наибольшее распространение получило шифрование данных. Банки, предоставляющие услугу Интернет-банкинга, применяют SSL-шифрование данных, передаваемых от

компьютера пользователя в систему банка и обратно. Данная мера безопасности исключает возможность открытой утечки личной информации клиента к третьим лицам.

Использование одноразовых СМС-паролей и «3-D Secure» кодов позволяет проводить аутентификацию пользователя в системе Интернет-банкинга. Каждая операция, совершаемая с помощью онлайн-банкинга, должна быть подтверждена одноразовым паролем, который приходит в СМС-сообщении на мобильный телефон. Преимущество данной системы в том, что злоумышленник не может завладеть паролем, существующим в течение короткого промежутка времени.

Еще одним распространенным способом установления аутентификации клиента онлайн-банкинга выступает электронная цифровая подпись, которая позволяет однозначно идентифицировать пользователя. Единственная возможность для злоумышленников при получении ключа от цифровой подписи – это заразить компьютер клиента вредоносным программным обеспечением. Специалисты рекомендуют чаще пользоваться антивирусными программами и регулярно проверять компьютер на предмет заражения компьютерными вирусами.

Помимо перечисленных выше мер защиты пользователей онлайн-банкинга банки применяют дополнительные меры для обеспечения безопасного пользования данной системы расчетов.

Среди них можно отметить ограничение использования личного сертификата (электронный ключ) – система некоторых банков позволяет использовать электронный ключ только на том компьютере, на котором он был сгенерирован. Таким образом, осуществлять платежи через Интернет-банкинг возможно только со своего личного компьютера. Не исключается возможность использования виртуальной клавиатуры, чтобы мошенники не могли «считать» регистрационные данные при вводе их с обычной клавиатуры с помощью компьютерных вирусов.

Большинство банков предусматривают в качестве меры противодействия несанкционированному проникновению к личным данным клиента ограничение длительности сессии: в случае неактивности пользователя, сессия в системе Интернет-банкинга через определенное время закрывается. Возобновление работы возможно только после новой аутентификации. Еще одним способом обеспечения безопасности является возможность использования истории подключений, с помощью этой функции пользователь Интернет-банкинга сможет отследить все несанкционированные операции, если они были произведены.

В заключение, обобщая вышеизложенное, необходимо отметить следующее. Обеспечение эффективной защиты личных данных и счетов в банке во многом зависит от самого пользователя, который должен нести самостоятельно ответственность за выполнение всех мер безопасности по защите своих данных.

В целях обеспечения эффективной безопасности в практике электронных расчетов необходимо использовать новые методы защиты. Считаем, что наибольшую эффективность могла бы привнести «токенизация», суть которой состоит в замене конфиденциального элемента на неконфиденциальный. Внедрение данного метода в систему Интернет-банкинга привело бы к повышению защиты.

Наравне с этим использование авторизации каждой онлайн-транзакции через клиринг и мониторинг мошеннических операций повысит эффективность контроля электронных расчетных операций посредством банковских платежных карточек.

УДК 343.985

Т.С. Сиделова, заведующий учебно-методическим кабинетом кафедры правовой информатики Академии МВД Республики Беларусь
sidelova@gmail.com

О ЦИФРОВОЙ ТРАНСФОРМАЦИИ УПРАВЛЕНИЯ САДОВОДЧЕСКИМИ ТОВАРИЩЕСТВАМИ

В настоящее время в Республике Беларусь насчитывается около 14,7 тыс. садоводческих товариществ, в деятельности этих организаций участвуют более полумиллиона граждан страны, а деятельность регламентируется рядом нормативных правовых актов, в том числе Указом Президента Республики Беларусь от 28 января 2008 г. № 50 «О мерах по упорядочению деятельности садоводческих товариществ».

В целом эта деятельность, основанная на самоорганизации граждан, носит положительный для общества характер. В то же время о несовершенстве правового и нормативного регулирования данной деятельности свидетельствуют многочисленные обращения членов садоводческих товариществ в органы государственного и местного управления. Эти обращения касаются в основном вопросов, связанных с нелегитимностью правления, принятием незаконных решений, не обоснованными размерами взносов и нецелевым их использованием, превышениями служебных полномочий председателями садоводческих товариществ, фальсификации протоколов общих собраний и иных документов, относящихся к ведению финансово-хозяйственной деятельности товарищества.

Несмотря на то что садоводческие товарищества являются некоммерческими организациями и создаются исключительно в целях пол-

ноценной реализации всеми членами товарищества предоставленных им прав и свобод, здесь не являются редкостью факты хищений и злоупотреблений служебными полномочиями. Председатели, члены правления, бухгалтеры и другие члены товарищества, которым были предоставлены управленческие функции организационно-распорядительного или административно-хозяйственного характера, осуществляют преступления экономической направленности: присвоение или растрата денежных средств, мошенничество, незарегистрированная предпринимательская деятельность на территории садоводческих товариществ, использование подложных документов при осуществлении финансово-хозяйственной деятельности, злоупотребление служебным положением, коммерческий подкуп, фальсификация документов. Все эти факты влияют на морально-психологическое состояние общества.

Обсуждение в средствах массовой информации, юридических изданиях проблем регулирования деятельности садоводческих товариществ подтверждает необходимость совершенствования регулирования деятельности данных юридических лиц.

Следует отметить, что использование традиционных подходов к контролю деятельности управленцев является затратным. Так, в диссертационном исследовании М.И. Парковской, выполненном в 2019 г., на тему «Особенности расследования преступлений экономической направленности, совершенных лицами, выполняющими управленческие функции в садоводческих некоммерческих товариществах», указывается на высокую сложность расследования подобных дел.

В то же время очевидно, что для решения комплекса социально-экономических вопросов и садоводческих товариществ необходимо упорядочить деловые процессы и сделать деятельность лиц, наделенных управленческими функциями, более прозрачной и доступной как для всех членов садоводческих товариществ, так и для работников органов местного управления и самоуправления.

На наш взгляд, сегодня одним из вариантов решения данной проблемы может стать нормативная регламентация, основанная на проработке основных процессов управления, их регламентации, создание электронной системы административного управления и учета деятельности садоводческого товарищества. Такая система должна иметь единый интерфейс и возможность удаленной идентификации с помощью подтвержденной учетной записи. Одним из компонентов этой системы должна быть система электронного дистанционного голосования, позволяющая членам садоводческого товарищества регистрироваться и голосовать путем заполнения электронной формы бюллетеня на сайте, знакомиться с повесткой собрания, материалами собрания, иными документами и объявлениями. С помощью данной электронной системы можно поддерживать онлайн-связь с председателем, членами правления, бухгалтером садоводческого товарищества, что позволит своевременно реагировать на проблемы, возникающие на территории садоводческих товариществ. Еще одним важным компонентом данной системы должна быть база данных, содержащая электронные документы (или электронные копии документов), относящиеся к финансово-хозяйственной деятельности садоводческого товарищества. Очевидно, что нормативно должен быть регламентирован доступ к базам данных системы и обеспечена безопасность хранения ее данных в облаке. Это позволит сделать деятельность товарищества более прозрачной и обеспечит возможность ведения делопроизводства в электронном виде, протоколирование деятельности товарищества, эффективного накопления и доступа к информации. Это, в свою очередь, в целом и облегчит разрешение споров, анализ хозяйственной деятельности садоводческого товарищества, проведение внутренних и внешних расследований, выявление неправомерных действий в этой деятельности.

Система электронного голосования усложнит фальсификацию протоколов голосования, минимизирует затраты на подготовку и проведение ряда мероприятий. В качестве примера приведем транзакционные издержки. Здесь затраты на организацию сбора участников при проведении общих собраний, аренду помещения, расходов на приобретение канцелярских товаров для отправки заказной корреспонденции являются значимыми. При этом будет соблюдаться прозрачность процедуры принятия коллективных решений членами садоводческих товариществ. Легитимность электронных коммуникаций позволит членам садоводческого товарищества голосовать в течение нескольких дней удаленно в любой период года и независимо от их местонахождения в любое удобное для них время суток.

В базе электронной системы возможно не только хранение протоколов общих собраний, управленческих решений и распоряжений управленцев, но и информирование о решениях местных органов власти по широкому кругу вопросов. Это обеспечит свободный доступ и ознакомление с ними всех членов садоводческого товарищества.

Таким образом, введение в практику и повышение качества самоуправления на базе технологий электронной демократии и создание электронной системы позволит сделать более эффективным управление садоводческим товариществом. Для управленцев, выполняющих управленческие функции в садоводческих товариществах, такие меры могут минимизировать число и последствия совершаемых преступлений экономической направленности.

УДК 334.024; 338.28

М.В. Тихомирова, аспирант Академии управления при Президенте Республики Беларусь
gromkovoinova@rambler.ru

О РАЗДЕЛЕНИИ РИСКОВ И ПРОБЛЕМ В СТРУКТУРЕ ЭЛЕКТРОННОГО ГОСУДАРСТВА

Создание и развитие структур и процессов электронного государства меняет характер взаимодействия государства и общества (Настельс, М. Информационная эпоха: Экономика, общество и культура / М. Настельс. – М., 2000. – 167 с.). В Беларуси эта проблема решается в рамках Государственной программы развития цифровой экономики и информационного общества на 2016 − 2020 годы (постановление Совета Министров Респ. Беларусь, 23 марта 2016 г., № 235). Однако, как показывает зарубежный опыт, оказание электронных услуг органами государственного управления порождает ряд не только положительных эффектов, но и формирует проблемы и риски. Сошлемся на административный опыт ЕС (Reorganization of government bask offices for better electronic public services-europian best practices, January 2004, DG Information Society, European Commission [Электронный ресурс]. – URL: http: //www.europa.eu.int/egovernment_research), а также научные исследования (Банасиковска, Я. Система отношений государства и общества в сфере государственных услуг в условиях цифровой экономики : дис. … д-ра экон. наук : 08.00.01 / Я. Банасиковска. – М., 2017. – 396 л.). С учетом зарубежного опыта в рамках белорусской модели государственного управления предлагается четко разделить эти две категории.

Риски связывают в первую очередь с неблагоприятными явлениями, порождаемыми несанкционированным использованием информационно-коммуникативными технологиями (ИКТ). Источником рисков при этом являются действия третьих лиц. Примерами таких явлений служат риски несанкционированного доступа к личным данным, частной жизни и коммерческой тайне получателей услуг; риски присвоения чужих имущественных и личных неимущественных прав посредством доступа в систему под чужим именем; мошенничество с использованием ИКТ; риски уничтожения или искажения информации в результате сбоев в системе или целенаправленной вирусной атаки и др. Перечень подобных примеров можно продолжить.

Под *проблемами* понимают неблагоприятные последствия для социально-экономического развития страны, порожденные новыми фор-

мами организации деятельности. Они вытекают не из преднамеренного противоправного поведения тех или иных лиц, а из характера и особенностей самой применяемой технологии. К числу примеров можно отнести цифровое неравенство пользователей, принадлежащих к разным поколениям, социальным группам, административно-территориальным единицам; электронную зависимость пользователей соответствующих услуг (привыкание к использованию электронных средств связи, хранения и обработки информации, электронных помощников, развлекательных систем); возможность оказания деструктивного информационно-психологического воздействия и др.

В приведенной ниже таблице систематизированы и разделены основные риски и проблемы, связанные с формированием и развитием системы государственных электронных услуг.

Таблица 3

Основные проблемы и риски системы государственных электронных услуг

№	Проблемы и риски	Категория	Источник
1.	Несанкционированный доступ к информации	Риск	Третьи лица
2.	Присвоение чужих прав	Риск	
3.	Уничтожение (искажение) информации	Риск	
4.	Цифровое неравенство пользователей	Проблема	Технологии
5.	Электронная зависимость	Проблема	

В целях внедрения и поддержки стабильного функционирования системы государственных электронных услуг (снижения как рисков, так и издержек) необходимы комплексные и целенаправленные усилия органов государственного управления. Перечислим основные меры, принимаемые на практике органами государственного управления в Республике Беларусь:

совершенствование законодательства и правоприменительной практики в области спецификации и защиты прав потребителей электронных услуг;

совершенствование организационной структуры государственного управления;

повышение доступности и прозрачности информации, направленное на смягчение проблемы асимметрии информации;

снижение издержек рентоориентированного поведения представителей власти;

издержки, связанные с преодолением последствий неверных решений, и т. д.

Сделаем некоторые выводы. На современном этапе развития экономики наблюдается широкое проникновение ИКТ в социальные технологии. Система государственных электронных услуг представляет собой комплекс услуг, предоставляемых государственными органами в соответствии с их компетенциями по запросу граждан, организаций или других государственных органов с помощью использования ИКТ посредством транзакций обмена. Внедрение системы государственных электронных услуг изменяет принципы отношений между государством, гражданами и предпринимателями. Граждане и организации получают более широкий доступ к информации о государстве, административных процессах, организациях и действиях конкретных представителей государства. В результате смягчается проблема асимметрии информации между участниками процессов, растет открытость органов власти, создаются условия для более действенного общественного контроля над деятельностью отдельных государственных служащих. Использование ИКТ при оказании государственных электронных услуг уменьшает большую часть транзакционных издержек. В то же время порождаются новые виды затрат и издержек: идентификации пользователей, защиты имени, защиты личной информации, интерпретации информации, потери (искажения) информации и др. В целом система государственных электронных услуг повышает эффективность государственного и местного управления, укрепляет доверие между государством, публичными образованиями, гражданами и организациями предпринимателей, стимулирует развитие экономики страны. В то же время оказание государственных электронных услуг порождает новые социальные проблемы и технологические риски, для преодоления которых необходимы совместные целенаправленные усилия общества и государства.

УДК 340.113:004

О.А. Федоренко, младший научный сотрудник лаборатории по проблемам противодействия преступности Национальной академии внутренних дел (г. Киев, Украины)
Kseniya25@ukr.net

ИНТЕРНЕТ ВЕЩЕЙ КАК УЯЗВИМОЕ МЕСТО ДЛЯ ДЕСТРУКТИВНЫХ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ

В настоящее время современный мир информационных технологий требует постоянного взаимодействия между своими компонентами. Однако люди имеют ограниченное время, внимание и точность. Все это означает, что человек – не лучший инструмент по сбору данных. В таких

условиях концепция коммуникации между устройствами предусматривает выполнение определенных действий вообще без вмешательства человека. Как следствие – вопрос разработки и внедрения технологий Интернет вещей активно обсуждается в Украине еще с конца XX в.

Понятие «Интернет вещей» (англ. Internet of things, IoT) рассматривается как сеть разнообразных объектов, увеличивается от промышленных устройств к потребительским товарам и услугам, которые могут обмениваться информацией и выполнять свои задачи.

Интернет вещей стремительно растет. По данным исследования консалтинговой компании, специализирующейся на рынках информационных технологий, Gartner по всему миру было 6,4 млрд подключенных вещей в 2016 г., что на 30 % выше, чем в 2015 г. В 2016 г. 5,5 млн новых вещей подключались к Интернету вещей ежедневно. С таким темпом, по прогнозу Gartner, к 2020 г. количество достигнет 20,8 млрд подключенных вещей.

Некоторые другие аналитические агентства выражают еще более оптимистичные прогнозы и предрекают 50 млрд подключенных устройств.

Высокий уровень неоднородности в сочетании с широкой гаммой систем IoT, как ожидается, увеличит число угроз безопасности владельцев устройств, которые все чаще используются для взаимодействия людей, машин и вещей в любой вариации. Традиционные меры обеспечения безопасности и конфиденциальности не могут быть применены к технологиям IoT, в частности, из-за их ограниченной вычислительной мощности.

Кроме того, большое количество подключенных устройств порождает проблему массовости. В то же время для достижения признания со стороны пользователей необходимо в обязательном порядке обеспечить соблюдение безопасности, конфиденциальность и модели доверия, которые подходят для контекста IoT. Для предотвращения несанкционированного доступа пользователей (т. е. людей и устройств) к системе должны использоваться механизмы аутентификации и авторизации, гарантированная безопасность, конфиденциальность и целостность персональных данных. По персональным данным пользователей и информации должны обеспечиваться защита и конфиденциальность, прежде всего потому, что устройства имеют к ней доступ и способны ей управлять (например, сведения о привычках пользователей).

Для Интернета вещей стоят сложные проблемы обеспечения безопасности по сравнению с теми, которые характерны для сетей связи. К ним добавляются возможные проблемы масштабируемости сети, вызванные мало предполагаемым объемом передачи данных от большого числа узлов, ненадежность программного обеспечения и т. п.

Широкое применение Интернета вещей – результат интеграции компьютерных технологий, технологий связи и различных областей промышленных отраслей. Кроме нарушения информационной безопасности традиционных сетей связи (в результате риска подслушивания, искажения информации, раскрытия информации) устройства и сети Интернета вещей сталкиваются с дополнительными проблемами безопасности на прикладном уровне – при использовании облачных вычислений, обработке информации, обеспечении прав на интеллектуальную собственность, защите приватности и т. д.

Угрозы для безопасности существующих сетей связи распространяются и на Интернет вещей, который построен на них. К ним относятся несанкционированный доступ, перехват данных пользователя, нарушения конфиденциальности, целостности информации, DoS-атаки, вирусы, эксплойты, сетевые черви и т. п. Кроме того, существуют межсетевые проблемы аутентификации, которые могут быть причиной DDoS и DoS-атак.

Распространение услуг IoT требует, чтобы были гарантированы безопасность и конфиденциальность. Таким образом, разрабатывая стратегию или политику по развертыванию систем Интернета вещей, следует учитывать сложность и относительную новизну этого явления, и вероятно возникновение непредвиденных социальных эффектов.

УДК 343.9

Э.Г. Хомяков, кандидат юридических наук, доцент кафедры криминалистики и судебных экспертиз Института права, социального управления и безопасности (ИПСУБ) Удмуртского государственного университета (УдГУ)
ed-18@yandex.ru

О СТАТИСТИЧЕСКОЙ ОТЧЕТНОСТИ, ДЕМОНСТРИРУЮЩЕЙ РЕЗУЛЬТАТЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Принятый в 1996 г. Уголовный кодекс (УК) Российской Федерации (РФ) в качестве одного из нововведений обозначил отдельную гл. 28 «Преступления в сфере компьютерной информации» (ст. 272–274). Революционная на тот период глава была введена как элемент противодействия новым видам преступлений, связанных с развитием информационных технологий.

Первые годы практической реализации положений данной главы, а именно раскрытия и расследования преступлений, предусмотренных ст. 272–274, позволили накопить необходимый опыт для борьбы с преступлениями «компьютерной направленности». Вместе с тем выявились и некоторые пробельные и проблемные моменты, не позволяющие говорить о наступательном противодействии указанному виду преступности со стороны различных правоохранительных структур, прежде всего МВД Российской Федерации. Возникли также проблемы в эффективном применении указанных статей УК РФ в различных субъектах Российской Федерации.

Накопленный опыт раскрытия и расследования преступлений в сфере компьютерной информации, а также тенденции в развитии информационных (компьютерных) технологий потребовали «ревизии» данной главы. В результате по истечении почти 15 лет с момента появления указанных видов преступлений был принят Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», в соответствии с которым гл. 28 была подвергнута изменениям.

Еще одно изменение гл. 28 претерпела в 2017 г., когда с принятием Федерального закона от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» появилась новая ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Основным субъектом расследования преступлений в сфере компьютерной информации согласно ст. 151 Уголовно-процессуального кодекса Российской Федерации являются следователи органов внутренних дел. Именно статистика МВД России дает наглядное представление о ситуации, возникшей на данном направлении борьбы с преступностью (см. табл. 4, 5).

Таблица 4

Количество преступлений в сфере компьютерной информации (гл. 28 УК РФ), зарегистрированных в Российской Федерации

Годы	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Количество преступлений	9 010	11 636	7 398	2 698	2 820	2 563	1 739	2 382	1 748	1 883	2 500

Таблица 5

Количество преступлений в сфере компьютерной информации (гл. 28 УК РФ), зарегистрированных по федеральным округам и городам федерального значения Российской Федерации (жирным шрифтом указаны максимальные показатели по отдельным годам)

Годы	Федеральные округа и города федерального значения Российской Федерации											
	Центральный	Северо-Западный	Северо-Кавказский	Южный	Приволжский	Уральский	Сибирский	Дальневосточный	Крымский	г. Москва	г. Санкт-Петербург	г. Севастополь
2008	2 377	333	–	257	**3 770**	516	701	533	–	1049	10	–
2009	2 929	282	–	217	**5 832**	1311	538	283	–	1164	16	–
2010	2 251	318	27	133	**2 498**	1150	454	348	–	666	16	–
2011	**980**	158	29	61	437	476	282	68	–	285	16	–
2012	**839**	246	28	70	669	420	263	103	–	324	33	–
2013	679	124	26	32	**693**	300	264	351	–	172	6	–
2014	**465**	162	30	37	413	231	178	60	3	109	13	1
2015	**1 027**	144	74	67	288	291	298	62	5	671	12	1
2016	**427**	158	49	54	408	245	320	46	6	164	13	1
2017	344	244	65	139	**502**	144	281	97	4	60	24	2
2018	385	383	42	192	**874**	214	234	129	4	59	8	2

Как видно из приведенных в табл. 4 данных, пик количества указанных преступлений пришелся на 2009 г., а затем после резкого падения в 2011 г. регистрационные показатели стабилизировались примерно на уровне 2000–2500 преступлений в год.

Показатели табл. 5 демонстрируют весьма разный подход к выявлению преступлений в сфере компьютерной информации в различных федеральных округах Российской Федерации. Явными лидерами в процессе выявления указанных преступлений являются Приволжский и Центральный федеральные округа; при этом на их фоне показатели отдельных округов выглядят весьма проблемными. Проблемными можно считать и показатели по городам федерального значения. И если правоохранительные органы в Москве в отдельные годы могли быть примером в выявлении и регистрации данных преступлений, то в последние годы ситуация сильно ухудшилась. Санкт-Петербург в этом отношении в рассматриваемые годы был явным аутсайдером.

Можно также отметить, что в Приволжском федеральном округе, где расположено 14 субъектов Российской Федерации, лидерами по регистрации преступлений в сфере компьютерной информации были Пермский край (в 2005, 2006 и 2012 гг.), Нижегородская область (в 2007, 2009, 2010, 2013, 2014 гг.), Чувашская Республика (в 2008 г.), Удмуртская Республика (в 2015–2018 гг.). Отдельные субъекты данного округа, не менее развитые в области использования современных технологий и по количеству населения не являющиеся последними, демонстрируют весьма посредственные результаты (Республика Татарстан, Самарская область, Саратовская область и др.).

Не менее значимы показатели по конкретным видам преступлений в сфере компьютерной информации (см. табл. 6).

Таблица 6

Количество преступлений в сфере компьютерной информации (ст. 272, 273, 274, 274.1 УК РФ), зарегистрированных в Российской Федерации

Годы	Статьи гл. 28 УК РФ			
	272	273	274	274.1
2008	7 450	1 543	17	–
2009	9 519	2 112	5	–
2010	6 309	1 089	–	–
2011	2 005	693	–	–
2012	1 930	889	1	–
2013	1 799	764	–	–
2014	1 151	585	3	–
2015	1 396	974	12	–
2016	994	751	3	–
2017	1 079	802	2	–
2018	1 761	733	5	1

Приведенные данные показывают, что ст. 274 УК РФ практически не работает, в то время как преступления, предусмотренные ст. 272 УК РФ, составляли в разные годы в среднем от 60 до 80 % в общем объеме зарегистрированных преступлений в сфере компьютерной информации. Но если данные о количестве зарегистрированных преступлений говорят об умении сотрудников органов внутренних дел выявлять указанные преступления, то данные, приведенные в табл. 7, демонстрируют их умения в раскрытии данных преступлений.

Таблица 7

Количество преступлений в сфере компьютерной информации (ст. 272, 273, 274, 274.1 УК РФ), зарегистрированных в Российской Федерации

Статьи УК РФ	Количество преступлений (зарегистрированных/раскрытых)				
	2014	2015	2016	2017	2018
272	1151/858	1396/716	994/529	1079/341	1761/319
273	585/462	974/483	751/373	802/385	733/254
274	3/1	12/13	3/1	2/0	5/1
274.1	–	–	–	–	1/0

Приведенные данные показывают, что в последние годы происходит снижение раскрытых преступлений, прежде всего по ст. 272 и 273 УК РФ.

Результаты официальной статистики очень часто весьма поверхностно раскрывают истинную ситуацию, сложившуюся по отдельным видам преступлений в Российской Федерации. Это связано прежде всего с огромным количеством показателей, которые остаются за рамками выводимых для всеобщего обозрения чисел.

Попытки интерпретации данной статистики в рамках научных исследований или официальных выступлений не всегда выглядят убедительно.

Например, назначенный в 2011 г. начальником Бюро специальных технических мероприятий МВД России генерал-майор полиции А.Н. Мошков в одном из выступлений заявил, что «снижение количества возбужденных уголовных дел по статьям 272 УК РФ … и 273 УК РФ … связано с уменьшением количества фактов доступа в сеть Интернет под чужими сетевыми реквизитами, так как благодаря усилиям Управления «К» МВД России провайдеры сети Интернет перешли на более взломоустойчивые технологии».

Следует иметь в виду и высокий уровень латентности преступлений в сфере компьютерной информации. Многие исследователи данного вопроса, ссылаясь на разные источники, отмечают, что в России латентность данных преступлений может достигать 90 %, т. е. 9 из 10 подобных преступлений либо не выявляются, либо не регистрируются правоохранительными органами.

Влияющими на статистику факторами могут также быть выявление в ходе расследования совокупности преступлений либо переквалификация преступления на разных этапах производства по делу (в связи с обнаружением новых сведений и фактов совершенного противоправного деяния или с появлением в уголовном законодательстве близких по ряду признаков составов преступлений). Так, с принятием в 2012 г. Федерального закона от 29 ноября 2012 г. № 207-ФЗ в УК РФ появилась новая статья 159.6 «Мошенничество в сфере компьютерной информации», а с 2017 г. отдельному учету стали подлежать преступления, совершенные с использованием компьютерных и телекоммуникационных технологий.

Существенный разброс в показателях регистрации преступлений в сфере компьютерной информации в разных субъектах Российской Федерации может быть связан также с недостаточной профессиональной подготовкой сотрудников, специализирующихся на расследовании данных преступлений, и отсутствием в их распоряжении необходимого методического материала (методик расследования, в том числе алгоритмов конкретных процессуальных, организационных и тактических действий на этапах выявления, регистрации, расследования указанных преступлений).

Несмотря на интенсивное развитие в России и за рубежом разнообразных информационных (компьютерных) технологий и, соответственно, появление новых видов преступлений, связанных с их использованием, необходимые учебные материалы, используемые для подготовки специалистов в области расследования подобных преступлений как в гражданских, так и в ведомственных вузах, часто отсутствуют. Например, в учебнике 2019 г. по криминалистике для бакалавриата под общей редакцией И.В. Александрова (Том 5. Методика расследования преступлений) раздел, посвященный основам методики расследования преступлений в сфере компьютерной информации, занимает 29 страниц; в учебном пособии 2019 г. «Криминалистическая методика» под общей редакцией А.Г. Филиппова данной тематике отведено 20 страниц; во многих учебниках и учебных пособиях по криминалистике, например, в учебном пособии 2019 г. «Криминалистическая методика» для академического бакалавриата под редакцией Л.Я. Драпкина данные вопросы вообще не рассматриваются.

Несомненно, изучение вышеперечисленных проблем, корректировка форм официальной отчетности, контроль за решением актуальных вопросов со стороны вышестоящих органов в расследовании преступлений в сфере компьютерной информации, изменение действующей нормативно-правовой базы, а также разработка необходимого учебно-методического материала позволит повысить эффективность как в борьбе с рассмотренными видами преступности, так и с новыми преступлениями, связанными со сферой информационных технологий.

УДК 004; 343.3/.7

В.Н. Цимбал, кандидат юридических наук,
старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России
sedruk@mail.ru

СОВРЕМЕННЫЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ВИДЫ, СПОСОБЫ СОВЕРШЕНИЯ И МЕТОДЫ БОРЬБЫ

Согласно статистическим данным ГИАЦ МВД России, за январь–сентябрь 2019 г. зарегистрировано более 205 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных

технологий, что на 69,2 % больше, чем аналогичный период прошлого года.

Почти половина подобных преступлений относится к тяжким и особо тяжким – 99 тыс. Средства, при помощи которых они совершаются: с использованием сети Интернет (108,5 тыс.), средств мобильной связи (78,5 тыс.), компьютерной техники (14 тыс.) и программных средств (4,5 тыс.).

Уголовное законодательство Российской Федерации (РФ) определяет преступления в сфере компьютерной информации в гл. 28, а именно 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», а также помимо вышеобозначенной главы к такого рода преступлениям относится ст. 159.6 «Мошенничество в сфере компьютерной информации».

Конвенция о преступности в сфере компьютерной информации ETS от 23 ноября 2001 г. № 185 предлагает государствам, подписавшим ее, рассматривать несколько групп таких преступлений: против конфиденциальности, целостности и доступности компьютерных данных и систем; связанные с использованием компьютерных средств; связанные с содержанием данных; связанные с нарушением авторского права и смежных прав.

Преступлений в сфере компьютерной информации, согласно указанным статистическим сведениям, за отчетный период всего зарегистрировано 2 577. По отдельным статьям данные следующие: ст. 159.6 УК РФ – зарегистрировано 533 преступления (-29,4 % по сравнению с АППГ), а раскрыто всего 49; ст. 272 УК РФ – зарегистрировано 1 683 преступления (+35,7 % АППГ), а раскрыто всего 343; ст. 273 УК РФ – зарегистрировано 354 преступления (-40,7 % АППГ), а раскрыто больше половины, а именно 185; по ст. 274 УК РФ – сведений нет.

Рассмотрим более подробно обозначенную категорию преступлений, основной отличительной чертой которых является компьютерная информация, под которой в примечании к ст. 272 УК РФ обозначается, что это «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Достаточно большое количество ученых (М.В. Самсонов, О.М. Иванова, С.А. Потапов, Н.А. Каменский, А.И. Халиулин, А.А. Васильев, К.Е. Демин и др.) изучало данное понятие и его значение. Достаточно глубокий анализ провел М.В. Старичков, который пришел к следующему выводу, что «компьютерная информация – это зафиксированные на материальном носителе сведения (сообщения, данные, команды),

представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначены для использования в таких устройствах». С данным мнением, на наш взгляд, стоит согласиться, так как обязательным условием совершения таких противоправных деяний и неотъемлемой его частью являются информационные технологии (компьютеры, средства связи и иное оборудование) и, конечно, информация, обращаемая в них.

Способы совершения компьютерных преступлений различны, выделим следующие:

кража носителя с компьютерной информацией или самого компьютера;

создание программ (компьютерные вирусы, сетевые черви, троянские программы), которые выполняют функции, причиняющие вред компьютерной информации (устройству и/или сети), например, хищение (удаление, модификация) данных, блокирование доступа, удаленное управление операционной системой или сетью, создание бот-сетей, распространение различной информации через зараженный компьютер, шифрование данных и т. п.;

мошеннические действия;

перехват информации;

удаленный несанкционированный доступ;

удаленные (сетевые) атаки: DoS-атаки, анализ трафика, «человек по середине», IP-спуфинг, атаки на уровне приложений и т. д.

комбинированные незаконные действия.

Из вышеуказанного следует, что способов совершения преступлений большое количество, также немало и орудий их реализации. Важными являются методы и применяемые средства для противодействия этим преступным деяниям, проведем некоторые параллели с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Методы борьбы с компьютерными преступлениями можем определить как технические, организационные (в ГОСТе – физический метод защиты), правовые и криптографические. На последнем пункте сильный акцент делать не будем, так как шифрование, как известно, является одним из самых эффективных способов защиты информации, при этом необходимо использовать соответствующее программное обеспечение (например, КриптоПРО) и аппаратные устройства. Применение пользователем криптографической защиты информации не позволит злоумышленнику использовать ее в корыстных и иных целях. Рассмотрим остальные методы подробнее:

1. Технические, т. е. обеспечение защищенности и безопасности компьютера или системы от возможного негативного воздействия при помощи различных программных и программно-технических средств,

а также мер, направленных на обеспечение бесперебойной их работоспособности. Например, использование легального и актуального антивирусного программного обеспечения, шифрование защищаемой информации, применение межсетевых экранов, обновление операционных систем и т. п.;

2. Организационные, т. е. обеспечение физической защищенности информации от ее получения злоумышленниками. Например, постоянное (своевременное, систематическое) обучение обычных пользователей, персонала организаций на предмет информационной безопасности, непренебрежение способами защиты: логины, сложные пароли, иные методы аутентификации, сохранение их в тайне; информирование пользователей о новых видах угроз и способах их реализации; помещение конфиденциальной информации в надежные хранилища и т. д.;

3. Правовые меры, т. е. разработка норм, правил, инструкций, определяющих методы и способы контроля эффективности защиты информации, обозначение ответственности за нарушения. Данная группа относительно эффективна: и уголовное законодательство РФ, и международные документы, и участие РФ в заседаниях международных организаций, которые, в свою очередь, уделяют большое внимание преступлениям в сфере компьютерной информации, киберпреступности и сотрудничеству государств в данной области.

Российской Федерацией признаются существующие проблемы в этой области и ведется следующая работа: в органах исполнительной власти созданы специальные подразделения (например, Управление «К» МВД России, Национальный координационный центр по компьютерным инцидентам, созданный ФСБ России), ведущие борьбу с компьютерными преступлениями; актуализируется законодательство РФ (например, в гл. 28 УК РФ в 2017 г. были внесены изменения, в Доктрине информационной безопасности РФ (указ Президента РФ от 5 декабря 2016 г. № 646) в разд. III компьютерные преступления обозначены как один из видов угроз безопасности страны); подготавливаются кадры для работы в данном направлении (различные учебные заведения); на постоянной основе проводятся дополнительное обучение, переподготовка и повышение квалификации в области информационной безопасности сотрудников различных органов и организаций, а также иная деятельность.

Подводя итог, отметим, что количество совершенных преступлений в сфере компьютерной информации растет, о чем говорят приведенные статистические данные. Происходит это, на наш взгляд, из-за бурного развития информационных технологий, их доступности как для обычного пользователя, так и для преступного элемента. Комплексность подходов по противодействию, борьбе с преступностью и минимизации возможного ущерба от их действий – залог успеха.

УДК 341.23:[343:004.9]

С.А. Чернышева, кандидат технических наук, доцент, профессор кафедры логистики и информационно-математических дисциплин, Минск, БИП – Институт правоведения
s_chernyshova@mail.ru

БОРЬБА С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ – КЛЮЧЕВОЕ ЗВЕНО В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На современном этапе развития информационного общества вопросы информационной безопасности в системе национальной безопасности государства приобретают первостепенное значение и охватывают практически все сферы жизнедеятельности человека.

Компьютерные преступления в контексте информационной безопасности представляют собой противоправные деяния, которые, кроме того, имеют международную природу благодаря устойчивому росту современных средств связи.

В Беларуси количество преступлений в сфере высоких технологий за пять лет стремительно возросло, наметилась устойчивая тенденция к увеличению количества зарегистрированных преступлений в этой сфере.

По данным МВД Республики Беларусь, в 2017 г. было зарегистрировано 3 999 преступлений, в 2018 г. – 4 741, а за 8 месяцев 2019 г. – 5 753 преступления, связанные с IT-технологиями. Такая динамика обусловлена ростом числа зарегистрированных в стране хищений путем использования компьютерной техники и осуществления несанкционированного доступа к компьютерной информации.

В настоящее время борьба с компьютерными преступлениями в сфере высоких технологий требует самого пристального внимания, анализа сложившейся ситуации и принятия конкретных радикальных решений.

Среди мер, направленных на эффективное улучшение ситуации, следует выделить образовательный аспект проблемы, а именно качественную подготовку специалистов нового направления, связанного с обеспечением информационной безопасности.

Так, в Академии МВД Республики Беларусь по инициативе Управления «К» началась подготовка по направлению «Противодействие киберпреступности и компьютерная разведка». Педагоги не только обучают специалистов для Управления «К», но и в целом вооружают сотрудников органов внутренних дел знаниями для борьбы с преступлениями, которые совершаются с помощью информационных техноло-

гий. Уникальный белорусский вуз первым в СНГ так подошел к решению вопроса цифровой грамотности сотрудников органов внутренних дел.

Курсанты новой специальности изучают международно-правовую базу и правовые аспекты информационной безопасности и защиты информации, универсальное и специализированное программное обеспечение, методы совершения преступниками противоправных деяний и т. д.

Основная часть занятий – практическая, проходит за компьютерами, а также в профильных службах ОВД. Курсанты приобретают также углубленные навыки по оперативно-разыскной деятельности в сети.

В свете рассмотренного выше, на наш взгляд, целесообразно включить в учебные планы всех специальностей современного образования, в том числе высшего, актуальную учебную дисциплину «Информационная безопасность и защита информации». Изучение данной дисциплины позволит сформировать у будущих специалистов различного профиля комплекс теоретических знаний, практических умений и навыков в области создания и управления системами информационной безопасности предприятий и организаций.

В заключение следует подчеркнуть, что транснациональность угроз в информационной сфере и уровень ущерба при их реализации ставят проблему обеспечения информационной безопасности как глобальную, требующую усилий всего мирового сообщества.

Государства мира уже давно осознали необходимость сотрудничества в борьбе с компьютерными преступлениями: принята Европейская конвенция о киберпреступности 2001 г., подписано Соглашение о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г., создана Международная специализированная организация по борьбе с кибертерроризмом «ИМПАКТ».

Однако проблемы единого подхода к киберпреступности остаются. Необходима разработка единых международных стандартов по юридическим, процессуальным и процедурным вопросам, которые позволяли бы классифицировать те или иные нарушения и принимать адекватные меры для их пресечения.

Выход из данного положения видится в заключении универсальной Конвенции по борьбе с киберпреступностью, разработке и подписании региональных договоров.

Усилия мирового сообщества должны быть направлены на разработку реальной стратегии интеграции в рамках глобального информационного общества.

УДК 378:004.9

Е.В. Чистая, преподаватель кафедры правовой информатики Академии МВД Республики Беларусь
843062@mail.ru

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ СРЕД В УЧРЕЖДЕНИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ В СООТВЕТСТВИИ С БОЛОНСКОЙ ДЕКЛАРАЦИЕЙ

В современном обществе наиболее актуальной становится подготовка специалиста, обладающего не только крепкими теоретическими знаниями, но и устойчивыми практическими навыками, для эффективной практической деятельности.

19 июня 1999 г. была подписана Болонская декларация, признанная урегулировать процесс сближения стран Европы в сфере высшего образования. В ней говорится: «Жизнеспособность и эффективность любой цивилизации обусловлены привлекательностью, которая ее культура имеет для других стран. Мы должны быть уверены, что европейская система высшего образования приобретает всемирный уровень притяжения, соответствующий нашим экстраординарным культурным и научным традициям». Россия присоединилась к Болонскому процессу в сентябре 2003 г. на берлинской встрече министров образования европейских стран. В 2005 г. в Бергене Болонскую декларацию подписал министр образования Украины. 14 мая 2015 г. в Ереване на Конференции министров образования стран ЕПВО и форуме по Болонской политике было объявлено о присоединении Белоруссии к Болонскому процессу и вступлении ее в Европейское пространство высшего образования. Одной из основных целей Болонского процесса является «содействие мобильности путем преодоления препятствий эффективному осуществлению свободного передвижения». В значительной мере этому будет способствовать унификация выдаваемых дипломов о высшем образовании, сходность специальностей и специализаций модульной системы образования, приведение к общим правилам перезачета сходных дисциплин.

Компьютерные сети и сети Интернет позволяют реализовать данные новшества в качестве модульной образовательной среды. Нужно обратить внимание на необходимость мультиязыковых сред для реализации электронных материалов. Реализация должна проходить не только на национальных языках, но и синхронизирована со странами, участвующими в Болонском процессе.

Особенно актуальной является не столько аккумуляция теоретической информации, сколько унификация между разными странами педа-

гогических методик и практик, а также образцов заданий, необходимых для специальностей и специализаций практических навыков, для выпуска учебным заведением высококачественных специалистов и профессионалов. Данные специалисты, в перспективе, должны быть задействованы не только в стране обучения, но и в странах, поддерживающих Болонский процесс гармонизации систем высшего образования.

Правильное структурирование материала для самообразования или использования данной информации в учебном процессе учреждений высшего образования является очень важным. Для этого актуально использовать обширные возможности компьютерных сетей и сети Интернет.

В использовании сети Интернет можно выделить следующие направления:

1. Комплектование учебных материалов в электронные учебно-методические комплексы (ЭУМК).

При создании ЭУМК и размещении их в сети Интернет необходимо использовать некоторую унификацию понятийно-терминологического аппарата национальных систем образования, так как в связи с болонскими соглашениями между странами должны существовать принципы гармонизации номенклатуры специальностей и квалификаций будущих специалистов. Инновационное обучение в странах тоже должно быть урегулировано с точки зрения программного обеспечения создания ЭУМК. Это в дальнейшем позволит присваивать учебным изданиям грифов учебно-методических объединений, а также организует обучающимся и профессорско-преподавательскому составу некоторую информационную среду для ориентирования в информационных компетенциях;

2. Информационно-образовательные сайты высших учебных заведений.

Ранее на сайте высшего учебного заведения предоставляли только информацию об административном ресурсе, часах и времени приемных дней различных отделов, факультетов, кафедр. В настоящее время этого недостаточно. В комплектацию сайта должны входить основные учебные компетенции, а также материалы для поступления в вуз, методические и информационные материалы, позволяющие и способствующие в дальнейшем обучающемуся легче ориентироваться в информации, необходимой для получения высшего образования. Сайты вузов в сети Интернет должны позволять поступающим сориентироваться в различных стадиях предоставляемых образовательных услуг не только в стране территориального расположения вуза, но и аналогичных специальностях и специализациях в странах, подписавших Болонскую декларацию. Необходимо обратить внимание на то, что сайты высших

учебных заведений, в соответствии с болонским процессом, должны быть реализованы на нескольких языках – не только на национальном языке, но и иностранных, зарегистрированных в качестве официальных в европейских высших учебных заведениях для перезачетов дипломов;

3. Образовательные сообщества на основании сайтов высших учебных заведений.

Наличие образовательных сайтов сходного профиля подразумевает под собой необходимость урегулирования образовательной информации по некоторым профилям. Актуально не только распределение по гуманитарным, техническим профилям, но и более узкоспециализированным специальностям и специализациям. Образовательные сообщества могут распределятся как и для решения некоторых узконаправленных научных задач, так и глобальных перспективных направлений в науке в целом. Пользователи таких сообществ могут объединить научные знания как национальной системы образования в данном направлении, так и перспективных направлений европейского научного сообщества;

4. Дистанционное образование.

Дистанционное обучение – форма получения образовательных услуг без посещения учебных заведений профессионального образования с помощью таких современных информационно-образовательных технологий и систем телекоммуникации, как электронная почта, телевидение и сеть Интернет. Повсеместное распространение компьютерной техники и системы Интернет позволяет реализовать возможность не только получать необходимую обучающую информацию, но и организовать общение, в том числе онлайн, между обучающимися и педагогическим составом. Можно организовывать также онлайн-семинары, называемые вебинарами, для непосредственного общения. В соответствии с приближением данного обучения к европейскому образованию актуально было бы делать на нескольких языках – национальном и английском.

Таким образом, использование возможности сети Интернет во всем многообразии перечисленных направлений, реализованных на основе компьютерных технологий, позволит перейти к новой парадигме эффективного обучения и самообразования. Это обеспечит не только должную информированность обучающихся в определенной области знаний, но и позволит обновлять полученные знания по специальности и специализации в дальнейшей практической профессиональной деятельности. Выпускники по данным специальностям и специализациям при правильной организации вышеперечисленных направлений подготовки будут востребованы не только в стране, в которой проходили обучение, но и во всех странах, подписавших Болонскую декларацию.

УДК 343.7

Д.И. Шнейдерова, преподаватель кафедры уголовного процесса и криминалистики учреждения образования «Могилевский институт МВД Республики Беларусь»
galuzodi@mail.ru

ХИЩЕНИЕ ЦИФРОВЫХ ВАЛЮТ КАК ВИД КИБЕРПРЕСТУПНОСТИ

Стремительное развитие информационных технологий способствует не только качественному преобразованию и упрощению жизни современного человека, но и появлению новых способов совершения хищений. Рост киберпреступности объясняется доступностью средств ее совершения (компьютеры, мобильные телефоны, сеть Интернет и др.), популярностью виртуального пространства и повышенным интересом к новым технологиям, а также сложностью и длительностью выявления и раскрытия такого вида преступлений.

К числу преступлений в сфере информационных технологий, к которым до недавнего времени относили распространение по локальным и глобальной сетям вредоносных вирусных программ и поддельных сайтов, взлом аккаунтов пользователей различных мессенджеров и социальных сетей с целью использования их личных данных в корыстных целях, завладение номерами банковских платежных карточек и др., добавился новый вид – хищение цифровых валют.

С момента вступления в законную силу Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» цифровые валюты, к которым приравнивается и криптовалюта с растущим числом ее видов, приобрели легализованный статус имущества, которые, как и любое другое имущество, могут быть отчуждены у своего владельца незаконным путем. При этом необходимо отметить, что законным владение криптовалютами будет считаться только при условии, если они были приобретены через зарегистрированные в Парке высоких технологий биржи. Однако официальная регистрация биржи и ее участников лишает их возможности оставаться анонимными, что противоречит принципам блокчейна, лежащего в основе распределительных систем, где и происходит «добывание» цифровых активов. Ввиду чего для совершения анонимных сделок пользователи выбирают в большинстве случаев любую из предлагаемых в сети Интернет распределительную базу, что лишает их средства правовой защиты.

Несмотря на вышеизложенное, риск быть обманутым и потерять внушительную часть реальных денежных средств, вложенных в цифровые валюты, присутствует в любой ситуации. Следует обратить

внимание на способы хищения криптовалют и токенов, получившие за последний год наибольшую популярность.

Большая часть криптоплатформ и бирж в качестве дополнительной защиты электронных хранилищ пользователей использует двухфазную систему безопасности, которая предполагает не только знание личного ключа, но и проверку пользователя посредством смс-оповещения с уникальным кодом для авторизации. Такая система заложила начало развития сим-свопинга, т. е. процедуры обмена сим-карт, который позволяет получить номер владельца электронного кошелька и код доступа к его цифровым валютам. Сим-свопинг включает в себя два этапа: получение логина криптокошелька и номера телефона пользователя, с последующим переводом его на новую сим-карту.

Активные пользователи социальных сетей и мессенджеров, пренебрегая безопасностью, публикуют свои персональные данные в открытом доступе в сети Интернет, привязывают аккаунты к номеру мобильного телефона, а также хранят персональные данные и пороли в файлах на различных носителях. Данное обстоятельство позволяет компетентным злоумышленникам получить необходимую информацию и использовать ее в корыстных целях, например, посредством вредоносных программ, внедряющихся на персональные устройства и копирующие личную информацию (логины, пароли, ключи и т. д.).

Второй этап сим-свопинга может вызвать затруднения, так как напрямую зависит от политики мобильного оператора. Чтобы перенести номер на новую сим-карту, прежде всего необходимо обратиться к оператору с просьбой о блокировке старой сим-карты, например, в связи с ее потерей или порчей. Следующий шаг – убедить оператора в необходимости перенести старый номер на новую сим-карту и выдать ее злоумышленнику. В данной ситуации возможно два варианта: если степень защиты данных пользователей мобильной сети низкая, то получение сим-карты возможно и без личного присутствия, например, по почте или курьером. В ином случае доступ к услугам оператора мобильной сети затруднен и возможен только через взаимодействие с недобросовестными сотрудниками компании. Используя сим-карту с номером пользователя, мошенник получает и доступ к его криптокошельку, откуда переводит на свой счет цифровые монеты и в последующем обналичивает их через любую криптобиржу на реальные деньги.

Существуют еще несколько вариантов доступа к электронным кошелькам через номер мобильного телефона. Так операторы мобильной связи предоставляют своим пользователям возможность управлять услугами через онлайн-сервис, где каждому номеру телефона отводится личный кабинет. Мошенник, получив доступ к такому кабинету, подключает услугу переадресации входящих смс-сообщений на свой

номер и тем самым имеет возможность перехватить уникальный код доступа к криптокошельку владельца. Стоит обратить внимание и на использование злоумышленниками специальных протоколов, которые позволяют отслеживать в мобильной сети поступающие на определенный номер смс-сообщения и информацию, содержащуюся в них, которая, соответственно, и дает возможность доступа к электронному криптокошельку и совершению хищения.

Среди мошенников пользуется популярностью метод фишинга, т. е. обмана пользователей путем создания поддельных сайтов, где владельцы криптокошельков добровольно вводят свои личные данные, используемые в последующем для совершения хищения. Фишинг может осуществляться как посредством рассылки писем на электронную почту, так и через создание чатов и открытых групп в социальных сетях и мобильных мессенджерах. Однако принцип механизма аналогичный в обоих вариантах: пользователь получает письмо или уведомление от имени криптоплатформы или биржи о необходимости пройти дополнительную авторизацию и прямую ссылку на сайт, переходя по которой попадает на идентичный настоящему по внешним признакам сайт мошенника. Следует отметить, что копированию подвергается даже доменное имя ресурса, в котором достаточно изменить всего один символ для его запуска. Доверчивый пользователь вводит необходимые злоумышленнику логин и пароль к своему криптокошельку, чем помогает последнему получить доступ к хранилищу и перевести все цифровые активы на сторонний кошелек. Кроме того, фишинговые сайты нередко ссылаются на рекомендации от знаменитых и влиятельных людей, которые как бы рекомендуют использовать именно этот сайт, как проверенный на личном опыте, что вводит неграмотных пользователей в заблуждение.

Еще один способ хищения криптомонет – внедрение вредоносного программного обеспечения (трояна), которое может быть загружено на устройство также посредством фишинг-атаки. Троян, попадая на незащищенное и уязвимое устройство, способен копировать всю информацию о системе и ее пользователе (его личные данные, информацию о банковских платежных карточках и счетах, логины и пороли к аккаунтам, ключи к криптокошелькам), с последующей передачей управляющему серверу, за которым и стоят мошенники, умело использующие полученные данные в корыстных целях.

Таким образом, перед правоохранительными органами стоит задача предупреждения и профилактики совершения такого рода хищений посредством пропаганды цифровой культуры в средствах массовой информации, сети Интернет или посредством личных бесед с гражданами и коллективами, которая должна включать в себя комплекс мер

по обеспечению безопасности личных данных пользователей при регистрации и использовании социальных сетей, мессенджеров и иных ресурсов сети Интернет.

УДК 343.4

Шукюров Шахин Тейюб оглы, доктор философии по праву, доцент кафедры «Административная деятельность в ОВД» Академии Полиции МВД Азербайджанской Республики
shahin 1967@mail.ru

КОНСТИТУЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ И ЕГО ВЗАИМОСВЯЗЬ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Компьютерная преступность – один из новых видов злостных правонарушений в нашем современном обществе. Она обладает характерными особенностями, среди которых способность быстро приспосабливаться к новым условиям и проникать во все сферы нашей жизни – ее главная цель.

В настоящее время преступления, совершаемые с использованием информационных технологий, создают особо глобальную угрозу национальной безопасности государств, открывают безграничные возможности, порождают все новые проблемы для развития общества. Информационные технологии в руках недоброжелателей служат удобным инструментом и быстро досягаемым рычагом для совершения других особо опасных видов преступлений, таких как терроризм, экстремизм, наркомания, тем самым создавая серьезные проблемы для его решений.

Несмотря на то что преступления, совершаемые с использованием информационных технологий, приобретают транснациональный характер, непосредственно находят свое глубокое отражение во внутренних делах государства.

На заседании Кабинета Министров Азербайджанской Республики, посвященном итогам 2013 г., Президент Азербайджанской Республики Ильхам Алиев, раскрывая характерные черты современной информационно-коммуникационной политики в государствах мира, отметил важную роль в формировании международного общественного мнения, расширяющихся с каждым днем интернет-ресурсов и транснациональных информационных систем, тенденцию перешагивания виртуальных связей через все национальные границы в мире. Президент Азербайджанской Республики особо подчеркнул, что на современном

этапе мирового развития одним из главных приоритетов национальной безопасности каждой страны является обеспечение информационной безопасности.

В обращении с ежегодным Посланием к белорусскому народу и Национальному собранию 21 апреля 2017 г. Президент Республики Беларусь А.Г. Лукашенко отметил следующее: «Обеспечение национальной безопасности невозможно без надежной защиты от деструктивных информационных атак, которые стали средством вмешательства во внутренние дела суверенных государств».

Конституционно-правовое обеспечение борьбы с компьютерной преступностью заключается в том, что Конституция – Основной Закон и акты, исходящие из него, устанавливая определенные права, свободы и обязанности граждан в сфере информационных отношений, запрещают выход за пределы указанных прав, свобод, обязанностей, а уголовное законодательство определяет уголовную ответственность за невыполнение требований содержания Конституции и законодательства.

Согласно содержанию конституций государств – участников СНГ в основном права и свободы граждан в сфере информационных отношений идентичны и основываются на конституционных принципах.

Право человека на информацию – одно из прав, закрепленных в действующих конституциях государств – участников СНГ. Допустим, это можно увидеть на примере Конституции Российской Федерации. Права и свободы человека и гражданина в сфере информационных отношений определены Конституцией Российской Федерации и включают в себя право доступа к информации, затрагивающей права, свободы и обязанности человека и гражданина; право на тайну частной жизни (ст. 23, 24), тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23); право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29); свободу слова (ст. 29).

В Конституции Азербайджанской Республики 12 ноября 1995 г. также закреплено положение о свободе слова, мысли и информации, право каждого гражданина на получение и распространение информации.

Конституции по своему содержанию также определяют ряд ограничений и запретов, связанных с информационными отношениями в целях правовой защиты ряда немаловажных институтов, таких как безопасность государства, оборона государства, личные права и интересы граждан, здоровье, государственный строй и др.

Кроме Основного Закона информационные отношения внутри государств – участников СНГ регулируются рядом актуальных документов: концепциями, программами, декретами и другими нормативными правовыми актами, тем самым предотвращая компьютерную преступность. Как указывают Ю.В. Полковниченко, Т.Г. Чудиловская в науч-

ной статье «Правовое регулирование в области информационных отношений в области информационной безопасности», правовое регулирование в области информационных отношений в Республике Беларусь осуществляется Законом Республики Беларусь «Об информации, информатизации и защите информации». Основной функцией данного закона является регулирование отношений, возникающих в процессе жизненного цикла информации, при создании и использовании информационных технологий, систем, сетей, ресурсов, а также при организации и обеспечении защиты информации. Важным документом, определяющим политику Республики Беларусь в сфере информационной безопасности, предотвращении компьютерной преступности является Концепция информационной безопасности Республики Беларусь от 18 марта 2019 г. В документе определены национальные интересы Республики Беларусь, внутренние и внешние источники угроз безопасности в информационной сфере, основные направления обеспечения информационной безопасности.

Следует отметить, что вопросы обеспечения информационной безопасности Азербайджана в общей форме нашли свое отражение в Концепции национальной безопасности от 23 мая 2007 г. и в Законе Азербайджанской Республики от 29 июня 2004 г. «О национальной безопасности». Политика информационной безопасности Азербайджанской Республики состоит в осуществлении комплекса мер, направленных на охрану государственных, общественных и частных информационных ресурсов, а также защиту национальных интересов в сфере информации.

Как указал А.М. Гасанов в монографии «Политика национального развития и безопасности Азербайджанской Республики»: «Проводимая в современном глобальном мире транснациональная политика в этой области создает в Азербайджане необходимость дальнейшего совершенствования правовых основ своей национальной политики информационной безопасности и повышения эффективности практической работы. По мнению экспертов, в современном мире обеспечение информационной безопасности каждой страны зависит от четкого определения приоритетов государственной информационной политики, точной, правильной, объективной, научно-теоретической оценки среды информационной безопасности и организации эффективной деятельности в этой области. Поэтому в настоящее время большое значение имеет определение и систематизация ключевых факторов, влияющих на среду информационной безопасности, и их отражение в отдельной Концепции Информационной Безопасности».

Развитие и совершенствование конституционно-правовых основ в области информационной безопасности создаст условия для обеспечения борьбы с компьютерной преступностью.

СОДЕРЖАНИЕ