Технико-криминалистическое обеспечение противодействия преступлениям против информационной безопасности объектов здравоохранения

Д.А. Степаненко[1], А.А. Рудых[2]✉

[1] *Байкальский государственный университет, г. Иркутск, Российская Федерация*
https://orcid.org/0000-0001-6844-8598; Research ID AAG-1755-2021; diana-stepanenko@mail.ru

[2] *отдел «К» ГУ МВД России по Иркутской области, г. Иркутск, Российская Федерация*
https://orcid.org/0000-0002-4015-1124; Research ID AAG-3797-2021; irkutianin38@gmail.com

АННОТАЦИЯ

В статье рассматриваются с криминалистических позиций отдельные виды преступных посягательств на информационные ресурсы учреждений здравоохранения. Приведены примеры использования вредоносного программного обеспечения в преступных целях. Описаны организационные, технические и правовые меры обеспечения информационной безопасности объектов здравоохранения. Сделан вывод о необходимости интеграции информационных ресурсов организаций здравоохранения в систему критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА

информационная безопасность; компьютерная информация; врачебная тайна; вредоносное программное обеспечение; критическая информационная инфраструктура; объекты здравоохранения; оказание медицинской помощи.

ДЛЯ ЦИТИРОВАНИЯ

Степаненко Д.А., Рудых А.А. Технико-криминалистическое обеспечение противодействия преступлениям против информационной безопасности объектов здравоохранения // Академический юридический журнал. 2021. Т. 22, № 1. С. 41–48. DOI: 10.17150/1819-0928.2021.22(1).41–48.

Criminalistic support for countering crimes against the information security of healthcare facilities

D.A. Stepanenko[1], A.A. Rudykh[2]✉

[1] *Baikal State University, Irkutsk, Russia*
https://orcid.org/0000-0001-6844-8598; Research ID AAG-1755-2021; diana-stepanenko@mail.ru

[2] *Department of the Main Directorate of the Ministry of Internal Affairs of Russia for the Irkutsk Region, Irkutsk, Russia*
https://orcid.org/0000-0002-4015-1124; Research ID AAG-3797-2021; irkutianin38@gmail.com

ABSTRACT

The article considers certain types of crimes against the information security of healthcare institutions from a criminalistics point of view. Examples of the use of malicious software for criminal purposes are given. Organizational, technical and legal measures to ensure the information security of healthcare facilities are proposed. It is concluded that it is necessary to integrate the information resources of healthcare organizations into the system of critical information infrastructure.

KEYWORDS

information security; computer information; medical secrecy; malicious software; critical information infrastructure; healthcare facilities; medical care.

FOR CITATION

Stepanenko D.A., Rudykh A.A. Criminalistic support for countering crimes against the information security of healthcare facilities. *Akademicheskiy yuridicheskiy zhurnal = Academic Law Journal*. 2021, vol. 22, no. 1, pp. 41–48. (In Russ.) DOI: 10.17150/1819-0928.2021.22(1).41–48.

© Степаненко Д.А., Рудых А.А., 2021

В настоящее время защищенность цифровой информации является важным компонентом информационной безопасности в целом. Особую актуальность этот вопрос приобретает, когда речь идет о безопасности объектов критической информационной инфраструктуры. Осознание этой важной проблемы на государственном уровне способствовало реализации организационных и правовых мер по упорядочению отношений в сфере обеспечения информационной безопасности. Так, в 2017 году был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»[1] (далее – Закон о безопасности). Согласно статье 2 указанного Закона «безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак», а к объектам критической инфраструктуры в названном Законе отнесены, помимо прочего, информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения.

На современном этапе технологического развития множество учреждений здравоохранения обзавелись информационными системами, в которых сведения, необходимые для обеспечения их нормального функционирования, представлены в виде компьютерной информации. Для регламентации развития информационных ресурсов Постановлением Правительства Российской Федерации от 5 мая 2018 года было утверждено «Положение о единой государственной информационной системе в сфере здравоохранения»[2]. Указанная информационная система сформирована в целях обеспечения эффективного управления в сфере здравоохранения, повышения качества оказания медицинской помощи, профилактики заболеваний и повышения информированности населения о здоровом образе жизни.

В составе государственной информационной системы предусмотрено функционирование 13 информационных подсистем, включающих в себя реестр электронных документов, реестр пациентов, реестр медработников и организаций, электронную регистратуру, систему мониторинга оказания высокотехнологичной медицинской помощи, систему контроля в сфере государственных закупок медицинских препаратов и т. д. Равным образом Положением установлены порядок и сроки предоставления в информационную систему информации, а также порядок обмена информацией и условия доступа к ней.

Кроме того, в рамках Федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» 14 августа 2020 года Министерством здравоохранения Российской Федерации утверждены «Методические рекомендации по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения»[3]. Таким образом, в единую информационную систему интегрированы информационные ресурсы и частных медицинских клиник.

Мы наблюдаем, как уходит в прошлое бумажное документационное обеспечение истории болезни человека – медицинские карты. На смену им приходят электронные карты и электронные больничные листы. Так, в декабре 2020 года вступил в силу новый порядок оформления и выдачи листов нетрудоспособности, утвержденный Приказом Минздрава России от 1 сентября 2020 года № 925н[4]. Порядок уточняет алгоритм применения и случаи, когда листок нетрудоспособности может быть оформлен не только в бумажном виде, но и как электронный документ. В нем прописаны процедура работы в информационной системе для оформления электронного больничного, порядок его формирования.

Уже сегодня результаты клинических, лабораторных исследований, включая мультимедийные материалы компьютерной томографии, рентгенологических и ультразвуковых исследований пациентов в виде компьютерной информации хранятся на серверах учреждений здравоохранения.

Кроме этого, активно внедряется роботизированная хирургия, где применяются автомати-

[1] О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26 июля 2017 г. № 187-ФЗ // Российская газета. 2017. 31 июля.

[2] О единой государственной информационной системе в сфере здравоохранения : Постановление Правительства РФ от 05 мая 2018 г. № 555 : (ред. от 19 дек. 2020). URL: http://government.ru/docs/32570/.

[3] ИПП «Гарант.Ру».

[4] Об утверждении порядка выдачи и оформления листков нетрудоспособности, включая порядок формирования листков нетрудоспособности в форме электронного документа : Приказ Минздрава России от 01 сент. 2020 г. № 925н // СПС «КонсультантПлюс».

ческие инструментальные системы для проведения медицинских операций под управлением программного обеспечения. Все перечисленное создает условия для эффективного и качественного оказания высокотехнологичной медицинской помощи.

Одновременно с этим, учитывая свойства цифровой информации, многократно возрастают риски ее несанкционированного уничтожения, модификации или распространения за пределы информационной системы. Например, в декабре 2020 года многие средства массовой информации сообщали о крупной утечке файлов, содержащих персональные данные пациентов московских клиник, переболевших COVID-19[5]. Так, судя по сообщениям, в сети Интернет были распространены данные около 100 тысяч пациентов. Распространенные файлы включали в себя следующие данные о пациентах: Ф.И.О., место проживания, контактный номер телефона, полис ОМС, дата рождения, диагноз и т. д. Этот инцидент стал возможен в результате нарушений требований информационной безопасности.

В ряде случаев неправомерное воздействие на информационные ресурсы медицинских организаций может привести к невозможности оказания своевременной медицинской помощи, включая нарушение нормального функционирования целых учреждений здравоохранения, что создает опасность для жизни и здоровья людей. Как отмечают некоторые исследователи, «использование в современной жизни общества высоких технологий в преступных целях особенно опасно еще и тем, что они становятся объектом пристального внимания преступных групп» [1, с. 744].

В последнее время, осознавая потенциально высокую ценность информации, преступники нацелились на информационные ресурсы учреждений здравоохранения. Нередко для организации компьютерных атак преступники используют вредоносное программное обеспечение в целях несанкционированного криптографического шифрования информации. В случае такой «удачной» атаки обладатель информации утрачивает возможность доступа к ней.

Так, в августе 2020 года преступники атаковали информационную сеть Свердловского онкологического диспансера с применением вредоносного программного обеспечения [2]. В результате совершенного преступления были временно утрачены данные с результатами биопсии ряда пациентов, которые не дублируются на бумажных носителях. За расшифровку данных преступники потребовали денежное вознаграждение. Аналогичным образом в 2017 году преступникам удалось зашифровать файлы сервера Светлогорской центральной районной больницы[6]. За расшифровку неизвестные потребовали выкуп в сумме 1 BTC (биткоин).

Подобного рода посягательства на информационную безопасность в сфере оказания медицинской помощи зафиксированы во многих странах. Например, в 2016 году компьютерная сеть Голливудского пресвитерианского медицинского центра (США) подверглась воздействию вируса шифровальщика[7]. Чтобы восстановить доступ к файлам, администрация учреждения была вынуждена заплатить преступникам 17 тыс. долларов США в виртуальной валюте биткоин. Примечательно, что преступники изначально требовали выкуп порядка 3,4 млн долларов США. И это лишь единичные примеры посягательств на информационную безопасность медицинских учреждений.

Механизм совершения таких преступлений основан на технологии криптографического преобразования компьютерной информации, которая повсеместно используется для защиты данных пользователей. Как мы ранее указывали, «обратной стороной законного использования указанных информационных технологий является возможность скрытного и эффективного совершения преступлений с использованием средств шифрования» [3, с. 207].

Для организации компьютерных атак преступники используют вредоносное программное обеспечение, которое автоматически запускает несанкционированные информационные преобразования в компьютерной системе жертвы. Вирусы-шифровальщики или, как еще их можно определить, «криптовирусы», или «программы-вымогатели» [4, с. 49], попадая в информационную систему, производят шифрование всей пользовательской информации или ее части (обычно файлов, имеющих распространенное расширение). После чего за выдачу ключа-дешифратора или специальной компьютерной программы, по-

[5] Больных COVID-19 выписали в интернет. В сети оказались личные данные 100 тыс. московских пациентов // Коммерсантъ. 2020. 10 дек. С. 9.

[6] Хакеры взломали сервер Светлогорской ЦРБ и требовали биткоины за расшифровку файлов // Белта. 2017. 17 июня. URL: https://www.belta.by/incident/view/hakery-vzlomali-server-svetlogorskoj-tsrb-i-trebovali-bitkoiny-za-rasshifrovku-fajlov-253154-2017/.

[7] Медицинский центр Лос-Анджелеса заплатил хакерам $17 000 выкупа // 3D News. 2016. 18 февр. URL: https://3dnews.ru/928572.

зволяющей восстановить доступ к пользовательской информации, преступники требуют выкуп. Для обеспечения сетевой анонимности и получения денежных средств жертв создатели криптовирусов и вымогатели используют криптовалюту.

Указанный способ использования криптовирусов преступниками позволяет их отнести к категории вредоносных компьютерных программ, создание, распространение и использование которых запрещено под угрозой уголовного наказания, предусмотренного статьей 273 Уголовного кодекса Российской Федерации[8] (далее – УК РФ). Следует отметить, что некоторые авторы относят криптовирусы к одной из ключевых угроз информационной безопасности последнего времени [5, с. 180].

Известно, что способ совершения преступления является важным элементом криминалистической характеристики преступления и отражает его функциональную сторону. В рамках криминалистического подхода к анализу способов совершения преступлений, связанных с созданием и использованием вредоносного программного обеспечения, необходимо рассматривать действия преступников на этапах подготовки, совершения и сокрытия преступления.

Так, подготовка и совершение компьютерной атаки на информационные объекты системы здравоохранения включает, как правило, совместную деятельность нескольких лиц. В рамках подготовки к рассматриваемому преступлению необходимо создать вредоносное программное обеспечение. Этим обычно занимаются лица из числа тех, кто имеет познания в программировании и криптографии в силу профессионального образования, опыта работы и т. д. Создаваемый вирус должен обладать свойством скрытности, обеспечивать реализацию информационных преобразований на компьютере жертвы незаметно для последней, чем и определяется его вредоносность [6, с. 12]. Кроме того, вирус не должен обнаруживаться антивирусным программным обеспечением, поэтому на данной стадии могут привлекаться лица, специализирующиеся на обеспечении скрытности и маскировки разрабатываемого программного обеспечения.

Выполнение всех этапов создания криптовируса включает его тестирование преступниками на контролируемых ими компьютерах или информационных системах. После «успешного» завершения испытаний реализуется следующий этап преступления – распространение криптовируса. Целью этого этапа является внедрение криптовируса в информационную систему организации здравоохранения. В рамках решения задач этапа распространения привлекаются, как правило, лица, обладающие знаниями в области социальной инженерии. Исследователи отмечают, что техники социальной инженерии сегодня используются в качестве основы для новых способов компьютерных преступлений [7, с. 24]. В рамках реализации данного этапа могут использоваться различные каналы заражения, однако самым распространенным является сервис электронной почты организации.

Преступники, изучая профиль жертвы, формулируют адресат, тему и содержание рассылаемых писем по электронной почте, в которых в качестве вложения могут прикрепляться файлы с вредоносным программным обеспечением. Методы социальной инженерии позволяют сформировать письма, которые провоцируют предполагаемую жертву открыть их для прочтения, сохранить вложение и попытаться с ним работать, что позволит незаметно внедрить и активировать криптовирус в компьютерной сети.

Для организаций системы здравоохранения преступники могут имитировать исходящие электронные письма от привычных адресатов. К таковым в этой сфере относятся: медицинские учреждения, органы государственной власти в сфере здравоохранения, а также в области надзора за этой деятельностью, лаборатории, коммерческие компании, состоящие в договорных отношениях с организацией-жертвой в связи с поставками лекарственных препаратов, медицинской техники и расходных материалов и др. Тема письма также подбирается в рамках привычной деятельности организации, например: «договор на поставку реактивов», «таблица результатов лабораторных исследований», «накладная за медицинские инструменты», «информационное письмо Росздравнадзора» и т. п.

Следует сказать, что для большей достоверности сообщения и повышения вероятности заражения информационной системы преступниками могут использоваться взломанные электронные почтовые ящики различных учреждений и лиц, с которыми организация здравоохранения состоит в электронной переписке. На данном этапе осуществления атаки могут привлекаться лица или использоваться «услуги» интернет-сервисов для обеспечения неправомерного доступа к компьютерной информации, что само по себе уже образует состав преступления, предусмо-

[8] Уголовный кодекс Российской Федерации : Федер. закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

тренного статьей 272 УК РФ. Совершение указанного преступления, как элемента подготовки к заражению информационной системы, открывает преступникам возможность попытаться совершить аналогичные действия в отношении тех адресатов, которые состоят в переписке с контролируемым почтовым ящиком и имеют, соответственно, определенный кредит доверия.

Кроме того, нередко преступники используют технологию «спуфинга» электронной почты, которая позволяет подделать адрес отправителя письма. В сети Интернет существует множество платных сервисов, которые могут подменять адреса отправителя электронной почты, что позволяет вводить в заблуждение получателя «фальшивых» писем.

Можно выделить несколько механизмов проникновения вредоносных программ в информационную систему, которые основаны на уязвимостях или нарушениях требований информационной безопасности:

– уязвимость клиента электронной почты;

– уязвимость операционной системы;

– уязвимость веб-браузеров;

– загрузка вредоносных компьютерных программ с веб-ресурсов;

– использование внешних зараженных носителей информации.

Программный код криптовируса, в зависимости от уровня компетенции его разработчика, может включать алгоритм нарушения работоспособности информационной системы и даже процесс самоуничтожения, который активируется после действий по несанкционированному криптографическому преобразованию пользовательских файлов.

Нередко преступники используют обфускацию, т. е. запутывают программный код используемого программного обеспечения. Мы согласны с теми авторами, которые относят эти действия к способам сокрытия следов неправомерного доступа и использования вредоносного программного обеспечения [8, с. 91]. Потому как эти методы позволяют злоумышленникам сокрыть часть следов преступных действий и в последующем воспрепятствовать идентификации вредоносного программного обеспечения.

После совершенной атаки множество файлов в информационной системе организации могут быть недоступны легальному пользователю. На компьютере жертвы, как правило, остается сообщение с инструкцией для расшифровки файлов и требованием выплаты вознаграждения за пароль или программу, позволяющую восстановить доступ к информации. Для подтверждения своих намерений преступники обычно предлагают жертве выслать им один небольшой зашифрованный файл. В ответ преступники присылают восстановленную информацию из этого файла. Это необходимо для того, чтобы жертва атаки и вымогательства могла убедиться в возможностях преступника по восстановлению информации и согласилась на выполнение требований вымогателей.

Анализ таких преступлений показывает, что криминальный интерес преступников к указанной категории информации связан с тем, что атакуемая информация имеет большое значение. Например, в условиях всемирной пандемии утрата базы данных с результатами лабораторных исследований проб пациентов на короновирусную инфекцию может привести к тяжким последствиям.

Кроме того, некоторые категории данных необходимы для оказания медицинской помощи, в том числе в случаях, не терпящих отлагательства. По этой причине администрация медицинского учреждения в случае компьютерной атаки оказывается в ситуации вынужденного согласия с требованиями вымогателей.

Следует также отметить, что доминирующая часть компьютерной информации, циркулирующая в информационных системах учреждений и организаций, осуществляющих медицинскую деятельность, является конфиденциальной и подлежит защите. Конституция Российской Федерации[9] (статья 23) гарантирует неприкосновенность и защиту личной тайны человека. В соответствии с Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации»[10] информация, содержащая сведения о диагнозе, результатах медицинских исследований, лечении, а также о факте обращения в медицинскую организацию, относится к врачебной тайне. Кроме того, в соответствии с Федеральным законом «О персональных данных»[11] к персональным данным относится любая информация, прямо или косвенно относящаяся к субъекту персональных данных, которая подлежит защите. Следует учитывать, что в указан-

[9] Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. (с изм., одобр. в ходе общерос. голосования 1 июля 2020) // Официальный-интернет-портал правовой информации. URL: http://pravo.gov.ru/.

[10] Об основах охраны здоровья граждан в Российской Федерации : Федер. закон от 21 нояб. 2011 г. № 323-ФЗ // Российская газета. 2011. 23 нояб.

[11] О персональных данных : Федер. закон от 27 июля 2006 г. № 152- ФЗ // Российская газета. 2006. 29 июля.

ных информационных системах обрабатывается специальная категория персональных данных, обработка которых разрешается только с письменного согласия субъекта этих данных.

Анализ механизмов внедрения вредоносного компьютерного обеспечения позволяет утверждать, что заражение вредоносным программным обеспечением информационных систем медицинских организаций осуществляется различными способами. К их числу можно отнести неосторожное использование персоналом сети Интернет и электронной почты на служебных компьютерах, переход по подозрительным ссылкам, содержащимся во входящих письмах и, как следствие, возможность внедрения и активации вредоносных файлов в сети организации. Эти же последствия могут возникать в случаях использования персоналом «зараженных» внешних носителей информации, а также по причине уязвимостей в используемом программном обеспечении.

Необходимо также учитывать вероятность случаев умышленных действий по внедрению вредоносного программного обеспечения со стороны лиц из числа работников организации или лиц, допущенных к информационной сети учреждения.

Предотвращение и раскрытие такой категории преступлений невозможно без анализа причин и условий, способствующих их совершению, что, собственно, и является одной из криминалистических задач расследования преступлений. В первую очередь, следует обратить внимание на роль потерпевшей стороны. Как справедливо утверждают некоторые исследователи, «...необходимо признать, что жертва способна «помочь» злоумышленникам в реализации преступных целей своим поведением, а также действиями и бездействиями» [9, с. 155].

Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»[12] на обладателя информации возложены обязанности по обеспечению ее безопасности. Нередко администрация медицинской организации пренебрегает безопасностью своих информационных ресурсов, что позволяет сделать их легкой добычей преступных посягательств.

Вместе с тем деятельность по предотвращению несанкционированного воздействия на компьютерную информацию учреждений здравоохранения обязательно должна включать в себя реализацию мер правового, организационного и технического характера.

К объектам, требующим обеспечения информационной безопасности, в организации здравоохранения относятся:

– программно-технические средства обработки информации;

– обрабатываемая информация;

– система передачи информации и система связи;

– используемое программное обеспечение;

– средства защиты информации.

Правовые меры обеспечения информационной безопасности в медицинской организации, владеющей информационными ресурсами, должны включать разработку перечня локальных нормативных актов в этой области. К таковым можно отнести: политику конфиденциальности медицинской организации; перечень сведений, относящихся к категории конфиденциальной информации; должностные инструкции для медицинского и обслуживающего персонала, предусматривающие обязанность по соблюдению мер информационной безопасности и ответственность за их нарушение; инструкции по работе с информационной системой, электронной почтой, съемными носителями информации, регламентирующие порядок и права пользователей, методические рекомендации по работе с информационной системой, перечень требований к персоналу, имеющему доступ к информационной системе и т. д.

Реализация организационных мер обеспечения информационной безопасности должна включать: определение перечней пользователей с делегированием прав в зависимости от уровня доступа; обучение персонала правилам информационной безопасности; внедрение парольной политики; назначение ответственных лиц за обеспечение требований информационной безопасности; выявление и фиксирование информационных инцидентов. Необходимо также обеспечить контроль доступа к компьютерной сети и его соблюдение в целях сокращения числа пользователей, имеющих возможность оказания негативного воздействия на информационные ресурсы организации.

Технические меры обеспечения информационной безопасности должны включать в себя работы по обеспечению непрерывного резервного копирования информации на безопасные электронные носители. Кроме того, обязательными условиями являются: использование актуального противовирусного программного

[12] Об информации, информационных технологиях и о защите информации : Федер. закон от 27 июля 2006 г. № 149-ФЗ // Российская газета. 2006. 29 июля.

обеспечения; фильтрация трафика (использование межсетевых экранов); сегментирование информации по категориям пользователей; использование процедур идентификации и аутентификации субъектов доступа; техническая и программная защита носителей информации; обеспечение управления доступом; ограничение программной среды и т. д.

Выполнение указанного комплекса мер обеспечит эффективное противодействие посягательствам на информационные ресурсы медицинских организаций и нейтрализацию угроз информационной безопасности. В свете криминалистической профилактики, по мнению Р.С. Белкина, такие меры могут выступать как средства защиты объектов посягательства и обеспечения благоприятных условий возникновения доказательственной информации [10, с. 87–88].

Созданные в организации программно-технические условия мониторинга работы программ и сетевых устройств, а также действий пользователей информационной системы, в случае возникновения информационного инцидента или совершения преступления обеспечат возможность восстановления хронологии событий и помогут понять функциональную сторону произошедшего криминального события, что, собственно, и представляет криминалистический интерес. Кроме того, принятие указанных мер поможет в случае совершения преступления свести общественно опасные последствия к минимуму.

Современная система обеспечения безопасности критической информационной инфраструктуры Российской Федерации находится в стадии формирования. По нашему мнению, одним из действенных шагов в обеспечении информационной безопасности учреждений здравоохранения является поэтапная работа в соответствии с Законом о безопасности по включению их информационных ресурсов в категорию «значимых объектов критической информационной инфраструктуры». Это позволит эффективно интегрировать указанные ресурсы в поле функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Ищенко Е.П. Преступления, совершаемые с использованием высоких технологий / Е.П. Ищенко, Н.В. Кручинина. // Всероссийский криминологический журнал. 2019. – Т. 13, № 5. – С. 740–746. – DOI: 10.17150/2500-4255.2019.13(5).740–746.

2. Старков М. Хакеры зашифровали данные пациентов в Свердловском онкодиспансере / М. Старков // Медвестник. – 2020. – 1 сент.

3. Рудых А.А. Криптография и криминалистика: современные проблемы и возможные пути решения / А.А. Рудых // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2. – С. 203–212.

4. Бахтеев Д.В. Криминалистическая классификация цифровой доказательственной информации / Д.В. Бахтеев // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сб. ст. Междунар. науч.-практ. конф. – М., 2018. – С. 44–49.

5. Тирранен В.А. Криптовирусы как актуальная угроза кибербезопасности / В.А. Тирранен // Уголовно-правовое воздействие и его роль в предупреждении преступности : III Саратовские уголовно-правовые чтения. – Саратов, 2018. – С. 179–185.

6. Ефремова М.А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ / М.А. Ефремова // Информационное право. – 2015. – № 3. – С. 12–16.

7. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц / Д.В. Бахтеев // Российское право: образование, практика, наука. – 2016. – № 3. – С. 24–26.

8. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Lex Russica (Русский закон). – 2019. – № 3. – С. 87–99.

9. Кравцов Д.А. Виктимологическая профилактика преступлений против собственности, совершаемых в сфере информационных технологий / Д.А. Кравцов, Н.Н. Маркелов // Современная юриспруденция: актуальные вопросы, достижения и инновации : материалы XX Междунар. науч.-практ. конф. – Пенза, 2019. – С. 155–157.

10. Белкин Р.С. Курс криминалистики / Р.С. Белкин. – 3-е изд., доп. – Москва : Юристъ, 2001. – 837 с.

REFERENCES

1. Ishchenko Ye.P., Kruchinina N.V. High-tech Linked Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 5, pp. 740–746. (In Russian). DOI: 10.17150/2500-4255.2019.13(5).740-–746.

2. Starkov M. Hackers encrypted patients' records in Sverdlovsk Oncologic Dispensary. *Medvestnik*, 2020, September 1. (In Russian).

3. Rudykh A.A. Cryptography and Criminalistics: Modern Problems and Possible Ways of Solution. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii = Vestnik of the Eastern Siberia Institute of the Ministry of the Interior of the Russian Federation,* 2019, no. 2, pp. 203–212. (In Russian).

4. Bakhteev D.V. Forensic Classification of Digital Evidentiary Information. In: *Criminalistics in the Conditions of Information Society Development (59th Annual Criminalistics Readings)*. Moscow, 2018, pp. 44–49. (In Russian).

5. Tirranen V.A. Cryptoviruses as Actual Cybersecurity Threat. In: *Criminal-Legal Impact and its Role in Crime Prevention. III Saratov Criminal-Legal Readings*. Saratov, 2018, pp. 179–185. (In Russian).

6. Efremova M.A. To the Question about Criminal Responsibility for the Creation, Dissemination and use of Malicious Computer Programs. *Informatsionnoe pravo = Information Law,* 2015, no. 3, pp. 12–16. (In Russian).

7. Bakhteev D.V. On the Modern Methods of Committing Fraud Against Individuals› Property. *Rossiyskoye Pravo: Obrazovaniye, Praktika, Nauka = Russian Law: Education, Practice, Researches,* 2016, no. 3 , pp. 24–26. (In Russian).

8. Rossinskaya E.R., Ryadovskiy I.A. Modern Means of Committing Computer Crimes and Patterns of their Execution. *Lex Russica (Russkii Zakon),* 2019, no. 3, pp. 87–99. (In Russian). DOI: 10.17803/1729-5920.2019.148.3.087-099.

9. Kravtsov D.A., Markelov N.N. Victimological Prevention of Crimes Against Ownership, Performed in Information Technologies. In: *Modern Jurisprudence: Current Issues, Achievements and Innovations. Materials of the XX International Scientific and Practical Conference*. Penza, 2019, pp. 155–157. (In Russian).

10. Belkin R.S. *A Course in Criminalistics*. 3rd ed. Moscow, Yurist Publ. , 2001. 837 p. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Степаненко Диана Аркадьевна – доктор юридических наук, профессор, профессор кафедры криминалистики, судебных экспертиз и юридической психологии Байкальского государственного университета; 664003, Россия, г. Иркутск, ул. Ленина, 11, e-mail: diana-stepanenko@mail.ru.

Рудых Алексей Александрович – кандидат юридических наук, начальник отдела «К» ГУ МВД России по Иркутской области; 664003, Россия, Иркутск, ул. Литвинова, 15, e-mail: irkutianin38@gmail.com.

INFORMATION ABOUT THE AUTHORS

Diana A. Stepanenko – Doctor of Law, Professor, Professor of the Department of Criminalistics, Judicial Expertis and Legal psychology. Baikal State University. Lenin st., 11, Irkutsk, Russian Federation, 664003, e-mail: diana-stepanenko@mail.ru.

Alexey A. Rudykh – PhD in Law, Head of the «K» Department of the Main Directorate of the Ministry of Internal Affairs of Russia for the Irkutsk Region. Litvinova st., 15, Irkutsk, Russian Federation, 664003, e-mail: irkutianin38@gmail.com.

Поступила в редакцию / Received 30.11.2020

Доработана после рецензирования / Revised 20.02.2021

Принята к публикации / Accepted 01.03.2021