Научная статья
УДК 343.98
DOI: 10.37973/KUI.2022.86.64.017

К ВОПРОСУ О ПРИМЕНЕНИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Салават Айратович Хамидуллин, МВД по Республике Татарстан, Казань, Россия
Альфия Васильевна Лебедева, Казанский юридический институт МВД России, Казань, Россия, lebserg@rambler.ru

Аннотация

Введение: в статье рассматриваются вопросы прикладного применения вредоносного программного обеспечения в деятельности оперативных подразделений в области противодействия преступлениям в сфере компьютерной информации.

Материалы и методы: материалами исследования послужили научные статьи, статистические данные Генеральной прокуратуры Российской Федерации за период с 2017 по 2021 г., Главного информационно-аналитического центра МВД России, интернет-источники. В работе применялась совокупность общенаучных и частнонаучных методов: описательный, метод логического осмысления, абстрагирование и обобщение, анализ, синтез, системный подход, статистический метод.

Обзор литературы: особое внимание уделено работам М.М. Долгиевой, А.Л. Мухина, С.М. Шухина, рассматривающих вопрос существующих анонимных сервисов в информационно-телекоммуникационной сети «Интернет». В исследованиях И.Н. Архипцева, А.В. Сарычева освещается проблема подготовки специалистов в ведомственных образовательных организациях МВД России по противодействию IT-преступлениям. В работе Р.А. Архипцева указывается на несовершенство современных способов противодействия преступлениям в информационно-телекоммуникационной сети «Интернет».

Результаты исследования: отмечается, что существующие способы и средства анонимизации деятельности злоумышленников в информационно-телекоммуникационной сети «Интернет» являются серьезным препятствием в раскрытии преступлений в информационной среде. Детально описываются такие способы анонимизации трафика, как TOR-браузер. Обращается внимание на возможности использования вредоносного программного обеспечения в качестве способа идентификации клиентской машины и личности злоумышленников.

Обсуждение и заключения: авторы приходят к выводу, что применение вредоносного программного обеспечения в рамках оперативно-технических мероприятий позволит своевременно деанонимизировать личность злоумышленников, совершающих преступления с использованием информационно-телекоммуникационной сети «Интернет». Предлагается при разработке учебных планов обучения в специализированных вузах системы правоохранительных органов особое внимание уделять формированию компетенций, необходимых для противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Ключевые слова: вредоносное программное обеспечение; противодействие IT-преступлениям; специализированное программное обеспечение; анонимизация трафика; оперативно-розыскная деятельность

Для цитирования: Хамидуллин С.А., Лебедева А.В. К вопросу о применении вредоносного программного обеспечения в деятельности оперативных подразделений по противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий, в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 3 (49). С. 139 – 146. DOI: 10.37973/KUI.2022.86.64.017

Scientific article
UDC 343.98
DOI: 10.37973/KUI.2022.86.64.017

MALWARE IN THE ACTIVITIES OF OPERATIONAL UNITS TO COMBAT CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND AGAINST COMPUTER INFORMATION

Salavat Ayratovich Khamidullin,
the Ministry of Internal Affairs of the Republic of Tatarstan, Kazan, Russia
Alfiya Vasilyevna Lebedeva, the Kazan Law Institute of MIA of Russia,
Kazan, Russia, lebserg@rambler.ru

Abstract

Introduction: the authors study applied usage of malicious software in operating units in IT crime prevention.

Materials and Methods: the materials of the study were scientific articles, statistical data of the Prosecutor General's Office of the Russian Federation for the period from 2017 to 2021, the Main Information and Analytical Center of MIA of Russia, Internet sources. The work used a set of general scientific and special scientific methods: descriptive, method of logical understanding, abstraction and generalization, analysis, synthesis, systematic approach, statistical method.

Literature review: special attention is paid to the works of M.M. Dolgiyeva, A.L. Mukhin, S.M. Shukhin, raising the issue of existing anonymous services in the information and telecommunications network of the Internet. Studies by I.N. Arkhiptsev and A.V. Sarychev highlight the problem of training specialists in departmental educational institutions of the Russian Ministry of Internal Affairs to counteract IT crimes. In the work of R.A. Arkhiptsev, it is pointed out that modern methods of combating crimes in the information and telecommunications network of the Internet are imperfect.

Results: it is noted that the existing ways and means of anonymization of malefactors' activity in the information and telecommunication network Internet are the serious obstacle for disclosure of crimes in the information environment. Such methods of traffic anonymization as TOR-browser are described in detail. Attention is drawn to the possibility of using malware as a way to identify the client machine and the identity of the attackers.

Discussion and Conclusions: the article concludes that the use of malware as part of operational and technical activities will allow timely de-anonymization of the identity of offenders who commit crimes using the information and telecommunications network of the Internet. It is suggested to pay special attention to the formation of competences necessary for counteraction to crimes, committed with the use of information-telecommunication technologies, when developing training curricula in specialized higher educational institutions of law-enforcement system.

Keywords: malware; counteraction to IT-crimes; specialized software; anonymization of traffic; operational and investigative activities

For citation: Khamidullin S.A., Lebedeva A.V. Malware in the Activities of Operational Units to Combat Crimes Committed with the Use of Information and Telecommunication Technologies and Against Computer Information // Bulletin of the Kazan Law Institute MIA of Russia. 2022. Vol. 13. No 3 (49). P. 139 – 146. DOI: 10.37973/KUI.2022.86.64.017

Введение

Поступательное развитие науки, техники, производительных сил, наращивание информационно-технологического потенциала оказывают влияние на процесс интеграции новых технических разработок в общественные процессы, позволяющие поддерживать и сопровождать многие сферы жизнедеятельности социума. В связи с этим научно-технический прогресс диалектически детерминирует изменения в характере трудовых отношений, формах взаимодействия участников общественного производства, обмена и другой общественно значимой деятельности.

Научно-техническая революция открыла новые способы и методы управления высокопроизводительными многоотраслевыми технологическими системами, в частности, появились информационно-телекоммуникационные сети, информационные технологии управления и иные виды технологических решений, призванные удовлетворять общественные нужды; однако, помимо полезных социальных видов взаимодействия общественных институтов, достижения технического прогресса используются в общественно вредных целях.

По данным Главного информационно-аналитического центра МВД России, в 2021 году было зарегистрировано 517 722 преступления, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,4% больше, чем за прошлый год. При этом за последние 5 лет количество преступлений в информационной среде выросло в 25 раз[1].

Материалы и методы

Материалами исследования послужили научные статьи, опубликованные в различных изданиях, статистические данные Генеральной прокуратуры Российской Федерации за период с 2017 по 2021 г., Главного информационно-аналитического центра МВД России за 2021 г., интернет-источники. В работе применялась совокупность общенаучных и частнонаучных методов: описательный; метод логического осмысления, позволивший последовательно изложить материал; абстрагирование и обобщение, призванные систематизировать факты и дать их толкование; анализ и синтез, обеспечившие достоверность выводов;

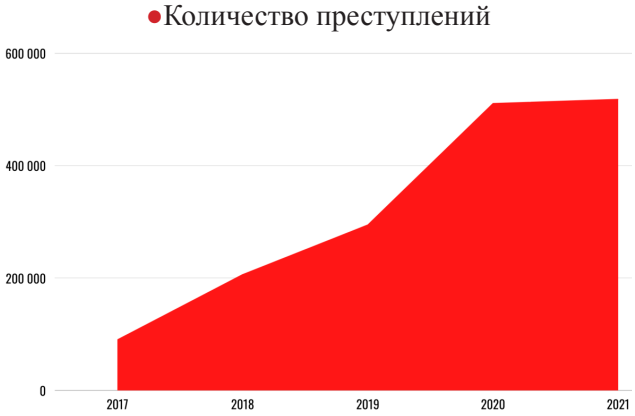

Рисунок. Количество киберпреступлений, зарегистрированных на территории Российской Федерации в 2017 – 2021 гг.[1]

Figure. Cybercrimes recorded in the Russian Federation (2017 – 2021)

системный подход, необходимый для раскрытия взаимосвязей между явлениями; статистический метод, использованный для анализа количественных показателей преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Обзор литературы

В настоящее время особенностям раскрытия преступлений, совершаемых в сети Интернет, посвящены научные труды М.М. Долгиевой [1], А.Л. Осипенко [2] и других. Ученые акцентируют внимание на использовании существующих IT-технологий в противоправных целях. На важность решения проблемы совершенствования методологии расследования преступлений в сфере компьютерной информации путем внедрения новых программных продуктов указывается в работе И.Н. Архипцева и А.В. Сарычева [3]. Авторы исследуют существующие проблемы в подготовке специалистов по раскрытию и расследованию преступлений в сфере компьютерной информации. Р.А. Дерюгин отмечает, что современные методы и способы противодействия, профилактики и предупреждения киберпреступлений отстают от современных способов противодействия им [4].

Результаты исследования

В настоящее время повышенную общественную опасность представляет киберпреступность,

[1] Киберпреступность в 2021 году выросла на 25%. URL: https://pravo.ru/news/232676/ (дата обращения: 15.03.2022).

[2] См.: Состояние преступности в России за январь–декабрь 2017 г. URL: genproc.gov.ru›upload/ iblock/aab…декабрь2017.pdf (дата обращения: 15.03.2022); Состояние преступности в России за январь–декабрь 2018 г. URL: genproc.gov.ru›upload/iblock/aab…декабрь2018.pdf (дата обращения: 15.03.2022); Состояние преступности в России за январь-декабрь 2019 г. URL: genproc.gov.ru›upload/iblock/aab…декабрь2019.pdf (дата обращения: 15.03.2022); Состояние преступности в России за январь–декабрь 2020 г. URL: genproc.gov.ru›upload/iblock/aab…декабрь2020.pdf (дата обращения: 15.03.2022); Состояние преступности в России за январь–декабрь 2021 г. URL: enproc.gov.ru›upload/iblock/aab…декабрь 2021 (дата обращения: 15.03.2022).

так как она характеризуется высокими темпами роста, по сравнению с иными формами преступности, и может нанести серьезный ущерб нормальному функционированию общественных институтов в России.

Криминогенный интерес к данной сфере преступной деятельности обусловлен многими факторами, одним из которых является утечка баз данных, в которых хранятся персональные данные пользователей онлайн-сервисов и платформ, а также коммерческая, профессиональная, врачебная, банковская и иная охраняемая законом тайна, получив доступ к которой злоумышленник может нанести существенный вред охраняемым законом интересам, начиная от простого хищения чужого имущества, заканчивая приостановлением деятельности крупных предприятий путем получения доступа к их информационным системам, дестабилизацией общественно-политической обстановки, работы служб жизнеобеспечения населения, а также оказанием иного деструктивного влияния на отраслевые стратегически и критически важные объекты Российской Федерации. Помимо этого, ситуация с киберпреступностью в настоящее время обостряется в связи с проведением специальной операции на Украине, послужившей катализатором для увеличения информационных атак на правительственные сайты и компании, находящиеся на территории Российской Федерации. Согласно данным Лаборатории Касперского, количество кибератак на российские компании в первые месяцы 2022 года выросло в 4 раза, по сравнению с аналогичным периодом прошлого года[1].

Следует отметить, что цифровые преступления по своей сути малоизучены и имеют высокий уровень латентности. Особый интерес в связи с этим представляют программное обеспечение и технические средства, позволяющие анонимизировать личность злоумышленников при совершении ими общественно опасного деяния посредством сети Интернет.

Согласно словарю С.И. Ожегова, «анонимным называется что-либо без указания имени того, кто пишет, сообщает о чем-нибудь без подписи»[2]. Определение, данное С.И. Ожеговым, можно также спроецировать и на современные реалии, однако с учетом некоторых особенностей.

Под анонимностью в сети Интернет подразумевается использование специальных технических и программных способов, маскирующих интернет-трафик и адрес технических средств в сети. Как правило, сокрытие соединений производится путем подключения через 2, 3, 5 и более IP-адресов по всему миру. Этот факт значительно затрудняет, а иногда делает невозможным установление реального IP-адреса злоумышленников.

Следует отметить, что одним из наиболее распространенных и эффективных программных средств, маскирующих сетевые пакеты обращения злоумышленников к доменам сети Интернет, является сеть TOR.

Анонимизация трафика обеспечивается за счет использования распределенной сети серверов на уровне onion-маршрутизаторов, что обеспечивает маскировку исходящих соединений, а также защиту анализа трафика, обеспечивая практически полную конфиденциальность действий в сети Интернет. Помимо этого, сеть TOR позволяет маскировать IP-адреса путем пропуска трафика пользователя через прокси-сервер на своей машине, обращаемого к серверам TOR, периодически образуя сетевую цепь с многоуровневым шифрованием исходящих пакетов.

Каждый такой пакет данных проходит через три различных прокси-сервера – сетевые узлы, которые определяются случайным образом.

Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего сетевого узла, потом для второго и в конце для первого. Когда первый узел получает пакет, он расшифровывает первый уровень шифруемой информации и направляет сетевые пакеты на следующие прокси-серверы. Второй и третий сервер поступают аналогичным образом. Указанные прокси-серверы работают на SOCKS-интерфейсе, что позволяет использовать для подключения к сети TOR программные продукты, основанные на том же принципе работы. К данному виду программного обеспечения можно отнести, например, браузер DuckDuckGO, который позволяет также оставаться анонимным в сети.

Для большей надежности злоумышленники работают с сетью TOR через соединения VPN, шифрующие интернет-трафик с использованием модемов, анонимных сим-карт, подключения к публичным DNS-серверам и других средств анонимизации личности. Помимо этого, для сокрытия деятельности в сети наиболее технически подготовленные злоумышленники посредством сканирования и использования уязвимостей, загрузки на технические средства жертвы эксплой-

[1] В России новые требования к кибербезопасности компаний. Как их выполнить. URL: https://pro.rbc.ru/demo/62b427879a7947025a54eb79?from=newsfeed?from

[2] Толкование и значение слова «анонимный». URL: https://ozhegov.textologia.ru/definit/anonimniy/ (дата обращения: 15.03.2022).

тов, руткитов и иного вредоносного программного обеспечения и иных способов получения удаленного доступа реализуют хакерские атаки через клиентские машины жертв.

При использовании указанной схемы установить личность злоумышленников путем направления запросов интернет-провайдерам и интернет-сервисам не представляется возможным, поскольку ответы, получаемые по международным каналам связи, направляются достаточно долго. В связи с этим получение компьютерной информации вследствие последовательной отправки запросов владельцам серверов, через которые проходил трафик злоумышленника, не дает результатов.

По мнению авторов статьи, для деанонимизации злоумышленников, совершающих преступления с использованием сети Интернет, необходимо внедрить практику прикладного применения вредоносного программного обеспечения (далее – вредоносное ПО) в рамках оперативно-розыскных и оперативно-технических мероприятий для решения проблемы идентификации лиц, подготавливающих, совершающих или совершивших общественно опасное деяние посредством использования сети Интернет.

Под вредоносным ПО следует понимать программный код, внедряемый на технические устройства жертвы для кражи паролей, получения доступа к файловой системе, причинения вреда либо изменения системных файлов на клиентских машинах жертв. Применение вредоносного ПО значимо тем, что при комплексном использовании в совокупности с иными программными средствами оно позволяет полностью исключить возможность обнаружения деятельности на технических средствах жертвы, что в результате дает возможность тайно и негласно получить всю представляющую интерес информацию, в частности, о личности жертвы, его контактных данных, текущем местоположении и т.д. Наиболее распространенными видами удаленного доступа к системе жертвы являются вирусы в форме троянов, бэкдоров и эксплоитов.

Одним из наиболее распространенных видов вредоносного программного обеспечения является бэкдор-вирус Glupteba-AFJK, являющийся подвидом трояна Glupteba. Данный вирус по своей сути до недавнего времени являлся вирусом-вымогателем, пока не был переделан и модернизирован в бэкдор, позволяющий получить доступ к компьютерной системе в целях проникновения либо внедрения иного вредоносного ПО. Помимо этого, в пример также следует привести разработанный иранской киберпреступной группировкой CharmingKitten бэкдор PowerLess, созданный на основе PowerShell-бэкдора, предназначенный для кибершпионажа путем загрузки в систему через расширяемое средство автоматизации[1]. Новый бэкдор PowerLess способен загружать и выполнять дополнительные модули, такие как инфостилеры и кейлоггеры, которые позволяют получить доступ к учетным данным жертвы, данным браузера и финансовой информации пользователя клиентской машины.

Особенность применения бэкдоров заключается в том, что их зачастую невозможно обнаружить в системе. Это обусловлено тем, что бэкдоры при их внедрении в систему автоматически перемещаются в автозагрузку клиентской машины жертвы и изменением файлов реестра. Из этого следует, что суть работы бэкдоров заключается в том, что они, проникая в систему, маскируются под исполняемые системные файлы, как, например, файл CL.exe, который является средством управления MicrosoftC++. Практически все бэкдоры являются резидентными, то есть активными во время работоспособности системы или в момент работы какого-либо программного обеспечения. Указанное свойство дает возможность самовоспроизводиться вредоносному ПО с каждой перезагрузкой системы, что обусловлено внесением изменений в значениях регистров клиентских машин. При этом основной целью бэкдоров является создание уязвимостей путем встраивания дефектов в алгоритмы работы системы, чтобы интегрировать на клиентскую машину жертвы другие типы вредоносного ПО. К подобным вредоносным программам относятся руткиты, кейлоггеры и другие типы вредоносного ПО, позволяющие получить доступ к данным, хранящимся на клиентских машинах, а также к их операционной системе и подключенным средствам ввода и вывода.

Таким образом, использование вредоносного ПО для обеспечения расследования по уголовным делам позволит получить данные по идентификации лиц, представляющих оперативный интерес, путем установки MAC-адреса клиентской машины, получения биометрических данных посредством удаленного подключения к веб-камерам, микрофону, а также фиксации иной представляющей интерес информации через систему ввода и вывода на технических устройствах.

Обнаружение и фиксацию технических устройств лиц, совершающих общественно опасные деяния посредством сети Интернет, следует

[1] Иранские хакеры CharmingKitten используют новый PowerShell-бэкдор в целях кибершпионажа. URL: https://www.securitylab.ru/news/529389.php (дата обращения: 15.03.2022).

производить исходя из оперативно-розыскной ситуации. Так, при совершении преступлений фигурант при своей невнимательности или неосторожности может оставить цифровые следы в форме IP-адресов, номеров телефонов, MAC-адресов устройств и других средств связи злоумышленников на сайтах, в социальных сетях и иных интернет-ресурсах. Указанные следы возможно получить в результате интернет-разведки открытых источников (OSINT) и методов социальной инженерии для логирования устройств злоумышленника с последующим выявлением его технических устройств и иных средств связи, социальных сетей, определения уязвимости клиентской машины, написания и отправки вредоносного ПО для получения доступа к системе.

Для разработки и прикладного применения вредоносного ПО наиболее подходящей является операционная система на базе Linux. Под Linux следует понимать семейство Unix-подобных операционных систем на базе ядра Linux, включающих тот или иной набор утилит и программ проекта GNU.

Следует отметить, что большая часть программных продуктов, предназначенных для сканирования и атак клиентских машин жертв, представлена в виде скриптов, написанных на различных языках программирования, в которых отсутствует графических интерфейс. По нашему мнению, для применения указанных программных продуктов наиболее удобными в использовании являются терминалы Unix-подобных систем, к которым, как было указано ранее, относится операционная система Linux.

Таким образом, указанная операционная система является наиболее предпочтительной и удобной для создания и прикладного применения вредоносного ПО в рамках реализации целей и задач оперативно-розыскной деятельности.

Следует отметить, что применение вредоносного ПО предполагает ограничение прав и свобод граждан. Использование вредоносного ПО влечет за собой ответственность в соответствии с действующим российским законодательством, что противоречит принципам и целям оперативно-розыскной деятельности. Однако если проанализировать нормы Уголовного кодекса Российской Федерации (далее – УК РФ), а также иных нормативных правовых актов, регулирующих применение оперативными подразделениями средств, изъятых из гражданского оборота, можно заключить, что использование предлагаемого программного решения возможно в качестве специального технического средства, предназначенного для негласного съема информации.

Так, в соответствии с п. 7 постановления Пленума Верховного Суда Российской Федерации от 25 августа 2018 года № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина», уголовная ответственность возникает, в случае если специальные технические средства были использованы с нарушением норм действующего законодательства, к которым, в частности, относятся нормы Федерального закона от 12 августа 1994 года № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ № 144)[1].

ФЗ № 144 регламентирует вопросы применения специальных технических средств, предназначенных для негласного получения информации (оперативной техники)[2]. Согласно ст. 6 ФЗ № 144 оперативным подразделениям разрешается использовать в ходе проведения оперативно-розыскных мероприятий информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде.

В соответствии со ст. 8 ФЗ № 144 применение оперативно-розыскных мероприятий, ограничивающих конституционные права и свободы человека и гражданина, допускается на основании судебного решения при наличии информации о признаках состава преступления, по которому производство предварительного следствия обязательно, либо о лицах, подготавливающих, совершающих или совершивших подобного рода деяния, а равно о событиях и деяниях, создающих угрозу военной, экономической, государственной, информационной либо экологической безопасности России. Этой же позиции придерживается А.Л. Осипенко[3]. Автор указывает, что такой способ деанонимизации злоумышленников возможно реализовать лишь в рамках оперативно-розыскного мероприятия «Получение компьютерной информации» с учетом принципов и задач опе-

[1] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда Российской Федерации от 25.08.2018 № 46. URL: http://www.consultant.ru/document/cons_doc_LAW_314616/ (дата обращения: 15.03.2022).

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 15.03.2022).

[3] Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления. URL: https://cyberleninka.ru/article/n/novoe-operativno-rozysknoe-meropriyatie-poluchenie-kompyuternoy-informatsii-soderzhanie-i-osnovy-osuschestvleniya (дата обращения:15.03.2022).

ративно-розыскной деятельности, предусмотренных ФЗ № 144, что, по нашему мнению, является справедливой позицией, так как данное оперативно-розыскное мероприятие предусматривает удаленный доступ к компьютерной информации посредством закладных устройств или специализированного ПО.

Таким образом, при соблюдении всех правил, предусмотренных законодателем в ФЗ № 144, а также при наличии соответствующего судебного решения оперативные подразделения могут применять специальные технические средства в виде вредоносного программного обеспечения для негласного получения компьютерной информации в рамках оперативно-розыскной деятельности.

Обсуждение и заключения

Подводя итог изложенному, необходимо отметить, что в специальной литературе недостаточно отражены вопросы использования специальных техничес ких средств и возможностей при раскрытии преступлений, совершенных с использованием информационно-телекоммуникационной сети «Интернет».

Изменение злоумышленниками IP-адресов, MAC-адресов клиентских машин, а также использование иных способов анонимизации в сети сводит поиск указанных лиц практически к минимуму.

По мнению авторов, применение вредоносного программного обеспечения в рамках оперативно-розыскных и оперативно-технических мероприятий позволит своевременно деанонимизировать злоумышленников в сети Интернет, что в результате увеличит эффективность деятельности оперативных подразделений при раскрытии преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Считаем необходимым разработать и ввести специальную дисциплину для обучающихся на очной и заочной формах обучения, а также дополнительную образовательную программу повышения квалификации для действующих сотрудников органов внутренних дел Российской Федерации в системе ведомственного образования правоохранительных органов по администрированию и прикладному применению Linux-систем, предназначенных для осуществления тестирования на проникновение, программных продуктов виртуализации, специализированного программного обеспечения, позволяющего сканировать клиентские машины или домены на имеющиеся уязвимости. Данное нововведение создаст условия для приведения в соответствие навыков оперативно-розыскной работы сотрудников органов внутренних дел Российской Федерации с информационно-телекоммуникационной средой, в которой совершаются рассматриваемая группа преступлений.

СПИСОК ИСТОЧНИКОВ

1. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109 – 115.

2. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы.и перспективы внедрения // Вестник Воронежского Института МВД России. 2015. № 2. С. 13 – 19.

3.Сарычев А.В., Архипцев И.Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий // Проблемы правоохранительной деятельности. 2020. № 1. С. 36 – 41.

4. Дерюгин Р.А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 1. С. 46 – 50.

REFERENCES

1. Deryugin R.A. Kiberprestupnost' v Rossii: sovremennoe sostoyanie i aktual'nye problemy // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. 2019. № 1. S. 46 – 50.

2. Dolgieva M.M. Kriptoprestupnost' kak novyj vid prestupnosti: ponyatie, specifika // Sovremennoe pravo. 2018. № 10. S. 109-115.

3. Osipenko A.L. Novye tekhnologii polucheniya i analiza operativno-rozysknoj informacii: pravovye problemy.i perspektivy vnedreniya // Vestnik Voronezhskogo Instituta MVD Rossii. 2015. № 2. S. 13 – 19.

4.Sarychev A.V., Arhipcev I.N. Sovremennoe sostoyanie raskrytiya i rassledovaniya prestuplenij, sovershaemyh s ispol'zovaniem informacionnyh tekhnologij // Problemy pravoohranitel'noj deyatel'nosti. 2020. № 1. S. 36 – 41.

Информация об авторах:
Хамидуллин Салават Айратович, оперуполномоченный отдела «К» МВД по Республике Татарстан

Лебедева Альфия Васильевна, кандидат экономических наук, доцент, доцент кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, lebserg@rambler.ru

Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:
Khamidullin Salavat A., Detective of the "K" Division of the Ministry of Internal Affairs of the Republic of Tatarstan

Lebedeva Alfiya V., Candidate in Economics (Research doctorate), Associate Professor, Associate Professor of Economics, Financial Law and Information Technologies in the Activities of Internal Affairs Bodies of the Kazan Law Institute of MIA of Russia, lebserg@rambler.ru

The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов:
Хамидуллин Салават Айратович – постановка проблемы, подготовка первоначального варианта текста статьи, работа с эмпирическим материалом, структурирование методической части статьи, формулировка выводов и практических рекомендаций, обобщение результатов исследования.
Лебедева Альфия Васильевна – общая концепция исследования, обобщение результатов исследования, научное редактирование и доработка текста статьи, подбор и анализ законодательных актов РФ, критический анализ материалов и выводов исследования.

Статья получена: 28.07.2022.
Статья принята к публикации: 16.09.2022.
Статья опубликована онлайн: 29.09.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаем.