МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

Методические рекомендации (памятка) сотруднику дежурной части при поступлении сообщения (заявления) о совершении дистанционного хищения (кибермошенничества)

Методические рекомендации

Казань
КЮИ МВД России
2023

ББК 67.4
М54

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты
Кандидат юридических наук **Д.Р. Мамлеева**
(Уфимский юридический институт МВД России)
Кандидат экономических наук **М.Н. Трофимов**
(Рязанский филиал Московского университета
МВД России им. В.Я. Кикотя)

Авторский вклад:
О.Г. Шмелева – инициация исследования, формирование общей идеи исследования, осуществление анализа и выводов исследования.
А.В. Лебедева, Л.Р. Назмеева, Д.Ф. Минзянова, Г.И. Хузяхметова – сбор аналитического и научного материала, подготовка первоначального варианта научного издания.

Шмелева О.Г.
М54 Методические рекомендации (памятка) сотруднику дежурной части при поступлении сообщения (заявления) о совершении дистанционного хищения (кибермошенничества): методические рекомендации / О.Г. Шмелева, А.В. Лебедева, Л.Р. Назмеева, Д.Ф. Минзянова, Г.И. Хузяхметова. – Казань: КЮИ МВД России, 2023. – 48 с.

В методических рекомендациях представлены основные направления деятельности сотрудников дежурных частей при получении сообщения о совершении кибермошенничества.
Методические рекомендации разработаны для преподавателей и курсантов (слушателей) образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ББК 67.4

Оглавление

Введение

Активное применение информационных технологий во всех сферах жизни общества является неотъемлемой характеристикой современности. Одной из главных проблем XXI в. выступает высокий рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий. С одной стороны, совершаются новые, ранее неизвестные преступления, с другой – преступники используют компьютерные технологии при совершении деяний, ответственность за которые уже закреплена в статьях Уголовного кодекса Российской Федерации, не регламентирующих преступления в сфере информационных технологий и компьютерных коммуникаций[1].

Средства телекоммуникаций и новые информационные технологии создают условия для подготовки, совершения и сокрытия хищений денежных средств с их использованием, к которым относятся: виртуальный характер дистанционных банковских операций; доступность открытых телекоммуникационных систем; высокая скорость выполнения транзакций; глобальный характер межсетевого операционного взаимодействия[2].

По данным официальной статистики, за период с января по июнь 2023 г. количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, составило 318 466, среди которых количество преступлений, предусмотренных ст. 159, 159^3, 159^6 УК РФ – 166 801^3.

Повсеместное внедрение во все сферы жизни общества современных информационных технологий приводит к еще более значительному росту компьютерной преступности, на который правоохранительные органы смогут адекватно отреагировать лишь

[1] Лебедева А.А. Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6. С. 49.

[2] Ревенков П.В. Управление рисками в условиях электронного банкинга: автореф. дис. ... д-ра эконом. наук. Санкт-Петербург, 2013. С. 20.

[3] Официальный сайт Министерства внутренних дел России. URL: https://xn--b1aew.xn--p1ai/folder/101762// (дата обращения: 21.07.2023).

при условии надлежащего правового обеспечения своей деятельности по противодействию преступности данного вида. Для успешного раскрытия и расследования таких преступлений сотрудникам ОВД необходимо тесное взаимодействие с другими службами, в том числе и в иностранных государствах. Также немаловажное значение приобретают квалифицированные действия оперативных дежурных, которые могут грамотно объяснить потерпевшему, как необходимо поступить в той или иной ситуации в целях сохранения следов преступления и улик.

Настоящие методические рекомендации будут способствовать выработке умений и навыков при прохождении первоначальной подготовки и повышения квалификации, а также повышению уровня профессиональной подготовки сотрудников дежурных частей при регистрации сообщений о кибермошенничестве.

Основные понятия и определения

DDOS-атака (Distributed Denial of Service, или «Распределенный отказ в обслуживании») – перегрузка информационной системы избыточным числом запросов, блокирующая обработку обращений[1]. Первостепенная задача DDOS-атаки – ограничение пропускной способности сервера, подключенного к сети Интернет с помощью отправления на него большого количества запросов[2].

DoS (от англ. Denial of Service – отказ в обслуживании) – атака, имеющая своей целью заставить сервер не отвечать на запросы. Такой вид атаки не подразумевает получение некоторой секретной информации, но иногда бывает подспорьем в инициализации других атак. Например, некоторые программы из-за ошибок в своем коде могут вызывать исключительные ситуации и при отключении сервисов способны исполнять код, предоставленный злоумышленником, или атаки лавинного типа, когда сервер не может обработать большое количество входящих пакетов.

DPaaS – Data Protection as a Service, Data Protection-as-a-Service – защита данных (ЗД) как услуга (как сервис), модель (технология) обеспечения сохранности данных DPaaS.

DSO – Data Security Officer – ответственный за безопасность данных, сотрудник, отвечающий за обеспечение безопасности обработки данных в системе и за противодействие попыткам несанкционированного к ним доступа и их использования.

False positive (FP) – 1. ошибочный допуск (к системе) – ложно положительная аутентификация, идентификация в ИБ – ситуация, когда средства биометрической аутентификации (биометрические, двухфакторные или иные) идентифицируют атакующего, злоумышленника или просто случайного человека как зарегистрированного пользователя и ошибочно разрешают ему

[1] DDoS-атаки: что это, происхождение, виды и способы защиты. URL: https://selectel.ru/blog/ddos-attacks/ (дата обращения: 02.06.2023).

[2] Галактионов Г.А., Шутов В.А. Противодействие DDOS атакам: методы и принципы защиты сайта РТУ МИРЭА // Инновации. Наука. Образование. 2021. № 46. С. 772.

доступ к ресурсам и данным компьютерной системы и сети, что является серьезным нарушением информационной безопасности.

High impact (HI, HIM, HIMP) – сильное воздействие, сильный эффект; высокая уязвимость, высокий риск, большой ущерб в ИБ – потеря или нарушение конфиденциальности, целостности или готовности, в результате чего можно ожидать серьезных или катастрофических последствий для работы организаций, для активов организаций, физических лиц, национальных интересов страны. Это может быть резкое снижение функциональных возможностей организации, уменьшение активов, большие финансовые убытки, тяжкие телесные повреждения или смерть людей.

IAM – это процесс управления идентификационными данными в цифровой среде компании. Он включает в себя управление идентификационными данными, аутентификацию, авторизацию и предоставление доступа. IAM крайне важна для любой организации, которая хочет сохранить контроль над своими данными, обеспечивая доступ к ним только авторизованных лиц.

IPv4 (англ. Internet Protocol version 4) – четвертая версия интернет-протокола (IP). Первая широко используемая версия. Протокол описан в RFC 791 (сентябрь 1981 года), заменившем RFC 760 (январь 1980 года).

IPv6 (англ. Internet Protocol version 6) – новая версия интернет-протокола (IP), призванная решить проблемы предыдущей версии (IPv4) при ее использовании в Интернете за счет целого ряда принципиальных изменений. Протокол был разработан IETF. Длина адреса IPv6 составляет 128 бит, в отличие от адреса IPv4, длина которого равна 32 битам.

IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) – сетевой адрес узла в компьютерной сети, построенный по протоколу IP. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети[1]. IP-адрес – это строка чисел,

[1] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких

разделенных точками. IP-адреса представляют собой набор из четырех чисел, например, 192.158.1.38. Каждое число в этом наборе принадлежит интервалу от 0 до 255. Таким образом, полный диапазон IP-адресации – это адреса от 0.0.0.0 до 255.255.255.255[1].

IP-спуфинг – распространенный вид атаки в недостаточно защищенных сетях, когда злоумышленник выдает себя за санкционированного пользователя, находясь в самой организации или за ее пределами. Для этого крэкеру необходимо воспользоваться IP-адресом, разрешенным в системе безопасности сети. Такая атака возможна, если система безопасности позволяет идентификацию пользователя только по IP-адресу и не требует дополнительных подтверждений.

Malware (от malicious software) – вредоносные (злонамеренные) программы, разг. мэлвер любая программа, скрытно введённая в компьютерную систему с намерением нарушить конфиденциальность, целостность или готовность её данных, приложений, ОС, т. е. действующая против интересов пользователя или владельца системы. К этой категории относятся все виды вирусов, черви, троянцы, шпионящее ПО, мэлвер для мобильных устройств (особенно для смартфонов) и т. п. Например, malware infection – заражение (инфицирование) вредоносным ПО.

Moderate impact (MI, MIM, MIMP) – умеренное воздействие, умеренный эффект; умеренная (средняя) уязвимость, умеренный риск, умеренный ущерб в ИБ – потеря или нарушение конфиденциальности, целостности или готовности, в результате чего можно ожидать не слишком серьезных последствий для работы организаций, активов организаций, физических лиц, национальных интересов страны. Это может быть снижение функциональных возможностей и эффективности работы организации, заметное

технологий: учебное пособие: в 2 ч. / А.В. Аносов и др. Москва: Академия управления МВД России, 2019. Ч. 1. С. 111.

[1] Что такое IP-адрес – определение и описание. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-an-ip-address (дата обращения 22.06.2023).

уменьшение активов, значительные финансовые убытки, телесные повреждения, но не смерть людей.

Penetration testing (также pentest, pentesting, penetration test, pen testing) – испытание проникновением, проф. пентест в ИБ – поиск уязвимостей и оценки безопасности компьютерной системы, веб-приложения, сети или хоста с помощью взлома, проводимый с разрешения владельца. Во время такого тестирования тестировщик, используя всю имеющуюся документацию (по архитектуре и реализации системы, по исходным текстам, по эксплуатации), устраивает псевдоатаку на корпоративную систему или компьютерную сеть, имитируя действия реальных злоумышленников, или атаку, проводимую каким-либо вредоносным ПО без непосредственного участия самого взломщика. Испытания проникновением существенно различаются по способу их организации. Существуют стандартизированные методологии проведения пентестов (GWAPT, IEM, OWASP). Итогом испытаний является письменный отчет с перечислением обнаруженных уязвимостей, уровня риска, связанного с каждой из них, и рекомендациями по снижению рисков. Такое тестирование должно проводиться периодически, поскольку изменения конфигурации сети, установка новых приложений и т. п. могут вызвать появление новых уязвимостей.

ping-флуд (от англ. ping-flood, дословно: наводнение запросами) – тип атаки на сетевое оборудование, ставящий своей целью отказ в обслуживании. Ключевой особенностью (по сравнению с остальными видами флуд-атак) является возможность осуществления атаки «бытовыми средствами» (программами и утилитами, входящими в состав домашних/офисных версий операционных систем).

SCTP (англ. Stream Control Transmission Protocol – «протокол передачи с управлением потоком») – протокол транспортного уровня в компьютерных сетях, появившийся в 2000 году в IETF. RFC 4960 описывает этот протокол, а RFC 3286 содержит техническое вступление к нему.

Secure web gateway (SWG) – защищенный веб-шлюз программная система, обеспечивающая защиту от внешних веб-угроз (web threat) – вредоносного и шпионящего ПО, нежелательного веб-контента, фишинга и т. п.

Spear phishing - это тип кибер-атаки, направленной на пользователей, имеющих доступ к корпоративным сетям. Это попытка обманом заставить сотрудников передать личную информацию, например, имена пользователей и пароли. Злоумышленники отправляют электронные письма, которые выглядят так, будто они исходят от законных источников, например, от компании.

SQL-инъекция – этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

TCP (англ. Transmission Control Protocol – протокол управления передачей) – один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами**.**

TCP/IP – сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается правилом (протоколом передачи). Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных, на которых базируется Интернет. Название TCP/IP происходит из двух важнейших протоколов семейства – Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были первыми разработаны и описаны в данном стандарте. Также изредка упоминается как модель DOD (Department of Defense) в связи с историческим происхождением от сети ARPANET из 1970-х годов (под управлением DARPA, Министерства обороны США[4]).

Threat space search (также threat-space search, TSS) – поиск (определение) пространства угроз (уязвимостей), поиск в

пространстве угроз ИБ – одно из средств обеспечения информационной безопасности (ИБ) и защиты системы от злонамеренных атак, а в некоторых играх – способ нахождения оптимальных решений (ходов), ведущих к выигрышу.

Threat window – окно опасностей, окно угроз в ИБ – время с момента появления уязвимости до момента ее устранения (иногда часы, дни или более длительный период) – и обновления базы данных известных угроз, вирусов, атак с соответствующими сигнатурами, которая обычно используется средствами (механизмами) защиты и позволяет снизить вероятность взлома системы, защитить ее от нового вида атаки. Если окно опасности открыто, злоумышленник может произвести успешную атаку на систему.

URL (Uniform Resource Locator) – интернет-адрес, присвоенный каждой web-странице. Каждый URL в Интернете уникален.

VPN или Virtual Private Network – это защищенный поток данных (туннель) между пользовательским устройством и сетью Интернет. Подключение VPN позволяет сберечь данные, передаваемые куда-либо, от стороннего влияния, а именно от прослушивания или вмешательства в них. Сервисы VPN являются наиболее простым способом по защите данных и сокрытия личных данных в сети Интернет[1].

Кибератака, атака из киберпространства (в киберпространстве) – атака, проводимая с помощью (специальных) программных и аппаратных средств на компьютерные сети и компьютерные системы противника с целью нарушения их работоспособности или для вредоносного управления компьютерным оборудованием/инфраструктурой, либо разрушения целостности данных или завладения информацией (данными). Кибератаки – политически мотивированные или направленные на достижение чисто финансовой выгоды, – являются инструментами и составляющими кибертерроризма (cyber-terrorism) и

[1] Что такое VPN и зачем это нужно? URL: https://www.kaspersky.ru/blog/vpn-explained/10635/ (дата обращения: 22.06.2023).

киберпреступности (cybercrime). Например, risk of cyber attacks – риск кибератак. Синонимы – cyber penetration, online attack.

Анонимус (транскрипция от англ. Anonymous, МФА: [əˈnɒn.ɪ.məs]; буквально – «анонимный», «аноним», «безымянный») – современная международная сеть активистов и хактивистов, отдельные узлы которой слабо связаны между собой.

Атака «человек посередине» – стороннее лицо осуществляет попытку получить несанкционированный доступ через сеть во время обмена данными. Подобные атаки увеличивают риски для безопасности такой конфиденциальной информации, как финансовые данные.

Атака подслушиванием – вид атаки, в которой атакующий вначале пассивно прослушивает обмен данными по протоколу аутентификации, чтобы собрать информацию, которую потом можно использовать для активной атаки, представляясь легальным претендентом на установление соединения.

Аутентификация – совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования, аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным.

Безопасность облака обозначает меры, которые организации применяют для защиты данных и приложений в облаке. Это важно для укрепления доверия клиентов, обеспечения отказоустойчивости операций и соблюдения правил конфиденциальности данных в масштабируемой среде. Надежная стратегия облачной безопасности предусматривает общую ответственность, распределенную между поставщиками облачных решений и организациями.

Ботнет (от англ. botnet; от robot и network) **–** компьютерная сеть, состоящая из нескольких зараженных устройств с запущенным

автономным программным обеспечением («ботами»). Компьютер становится «ботом» в составе ботнета после скрытой, самопроизвольной установки программы, позволяющей преступнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используется для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании[1].

Браузер – клиентская программа для работы во Всемирной паутине (WWW). Самые распространенные браузеры: Google Chrome, Mozilla Firefox и Opera.

Браузерный эксплойт («атака браузера» или «незапрашиваемая загрузка») – это форма вредоносного кода, которая использует уязвимость в браузере или компоненте системы с целью изменить настройки без ведома пользователя.

Веб-прокси (англ. web proxy) – это прокси-сервер и анонимайзер особого вида, представляющий собой веб-приложение (чаще всего PHP или Perl скрипт) установленное на веб-сервере, выступающее в роли посредника для загрузки контента различных веб-сайтов.

Веб-прокси могут быть использованы для следующих целей:

- ускорения загрузки веб-сайтов;
- тестирования онлайн-сервисов;
- обхода ограничений администратора локальной сети на доступ к определенным адресам веб-сайтов;
- сокрытия реального IP-адреса и анонимного доступа к веб-сайтам;
- получения доступа к веб-сайтам закрытым для просмотра пользователей определенных стран;

и многих других целей.

Вредоносная программа – это любое программное обеспечение, которое осуществляет несанкционированный доступ

[1] Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. Москва, 2018. С. 23.

и/или воздействие на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа[1].

Вредоносные утилиты – вредоносные инструментальные программы, программы, предназначенные для автоматизации создания вирусов, червей или троянских программ, DoS-атак на удалённые серверы, взлома других компьютеров и т. п. В отличие от вирусов, червей и троянских программ, вредоносные утилиты сами не представляют угрозы для компьютера, на котором исполняются, а вредоносные действия выполняются приложением только по прямому указанию злоумышленника.

Высокотехнологичное преступление; высокотехнологичная преступность – категория преступлений, связанных, в частности, с современными информационными технологиями, особенно с Интернетом, – это, например, распространение разнообразных вирусов, хакерские атаки, направленные на незаконное получение конфиденциальной, в том числе финансовой, информации, дезорганизацию работы банков, корпораций, государственных учреждений и т. п. Синонимы – computer crime, cybercrime, electronic crime, e-crime.

Дистанционное мошенничество[2]:

- мошенничество, совершенное с использованием средств сотовой связи и сети Интернет. Предлоги, которые используют преступники, разнообразны и являются только условием для получения информации о банковской карте, счете или способствуют перечислению самим потерпевшим денежных средств на используемые мошенниками расчетные счета (такие как разблокировка банковской карты, приобретение и реализация товаров на интернет-площадках, в случаях, когда размещенный на них товар – только предлог для звонка потенциальному потерпевшему, компенсация за ранее приобретенные медицинские препараты, компенсация от Пенсионного фонда и т.д.).

[1] Вредоносное программное обеспечение. URL: https://ru.malwarebytes.com/malware/ (дата обращения: 20.11.2022).

[2] Кудрявцев Р.В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218 – 221.

• мошенничество, совершенное с использованием средств сотовой связи и непосредственного контакта с потерпевшим. Как правило, данный способ характерен при использовании предлога: родственник попал в беду, ДТП, полицию и т.д.).

• мошенничество, совершенное только с использованием интернет-ресурсов. Покупка, продажа товара на различных интернет-площадках, в том числе использование «зеркальных» сайтов (сайтов, схожих с оригинальными, которые принадлежат известным организациям), взлом страниц в социальных сетях и рассылка от имени пользователя страницы в социальной сети просьбы перечислить деньги.

Доверенная компьютерная система, безопасная (защищенная) система в ИБ – система, в которой реализован комплекс мер информационной и физической защиты согласно принятой политике обеспечения безопасности, что позволяет использовать ее для одновременной обработки разной чувствительной (конфиденциальной) или секретной информации.

Доверенный тракт, доверенный канал (взаимодействия) в ИБ – механизм, позволяющий пользователю или оператору (при помощи устройства ввода данных) непосредственно взаимодействовать (при соблюдении требований безопасности) с функциональными блоками защиты компьютерной системы или иного целевого объекта для поддержки принятой политики безопасности этой системы или объекта.

Домен – область пространства иерархических имен сети Интернет, которая обслуживается набором серверов доменных имен DomainNameSystem и централизованно администрируется[1].

Доме́нная зона – совокупность доменных имен определенного уровня, входящих в конкретный домен. Например, зона wikipedia.org включает все доменные имена третьего уровня в этом домене. Термин «доменная зона» в основном применяется в технической сфере, при настройке DNS-серверов (поддержание зоны, делегирование зоны, трансфер зоны).

[1] Семенова Т.В. Домен и доменное имя: отличия в правовом регулировании // Вестник Полоцкого государственного университета. 2019. № 13. С. 120.

Доменное имя – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет[1]. Первая группа символов в доменном имени обозначает домен первого (верхнего) уровня, расположенная перед ней – доменное имя второго уровня и т.д. Например, у домена первого уровня «.COM» (доменная зона «.COM») может быть доменное имя второго уровня «TELE.COM», у доменного имени второго уровня «TELE.COM» могут быть доменные имена третьего уровня «SOFT.TELE.COM» и «HARD.TELE.COM» и т.д. Поскольку доменное имя читается слева направо, оно, таким образом, последовательно называет уровни – от самого низкого к самому высокому[2].

Единая система идентификации и аутентификации (ЕСИА) – федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Емейл-бомба (англ. email-bomb) – простой способ кибератаки, суть которого заключается в нарушении нормальной работы электронной почты адресата при помощи отправления его почтового адреса сообщениями большого объема или в больших количествах. Является одним из вариантов DoS-атаки[1], может осуществляться многократной отправкой одного и того же сообщения. Для тех, кто пользуется платными почтовыми сервисами, такая атака может привести к повышению их стоимости.

Защита файла (файлов) в ИБ – совокупность процессов и процедур, призванных предотвращать несанкционированный доступ, заражение (инфицирование), удаление, модификацию или разрушение файла или каких-либо частей его контента;

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[2] Матвеев Д.И. Использование товарного знака в доменном имени // Проблемы правовой информатизации. 2006. № 2. С. 25.

обеспечивается на уровне ОС путем разделения (разграничения) прав доступа.

Идентификация – совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица[1].

Инсайдерская угроза – это угроза, которая исходит от людей внутри организации, например сотрудников с недобрыми намерениями. Сотрудники обладают высоким уровнем доступа к компьютерным системам и могут дестабилизировать безопасность инфраструктуры изнутри.

Интернет – всемирная система объединенных компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных[2].

Интернет вещей (IoT) – обозначает электронные устройства, работающие удаленно в Интернете. Например, умный будильник, отправляющий регулярные обновления на смартфон, считается устройством IoT. Устройства IoT создают дополнительный уровень рисков для безопасности из-за постоянного подключения и скрытых программных ошибок.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[3].

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[2] Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. Москва, 2018. С. 20.

[3] Организация данных в системах обработки данных. Термины и определения: ГОСТ 20886-85. URL: http // docs.cntd.ru/document/1200015708 (дата обращения: 10.06.2023).

связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[1].

Информационные технологии (согласно определению, принятому ЮНЕСКО) – это комплекс взаимосвязанных, научных, технологических, инженерных дисциплин, изучающих методы эффективной организации труда людей, занятых обработкой и хранением информации; вычислительную технику и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также связанные со всем этим социальные, экономические и культурные проблемы[2].

Информационный накопитель – устройство записи, воспроизведения и хранения информации.

Информационный носитель (носитель данных) – материальный объект, предназначенный для записи и хранения данных 5 (диск, лента, твердотельный носитель)[3].

Информация – сведения (сообщения, данные) независимо от формы их представления[4].

Кейлоггеры записывают каждое нажатие клавиш пользователя, включая банковские реквизиты, пароли от социальных сетей и т.д. Они подразделяются на аппаратное и программное вредоносное обеспечение. Наиболее распространены программные кейлоггеры, встраиваемые в операционную систему компьютера, что делает их невидимыми. Клавиатурные шпионы чаще всего являются частью

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[2] Бакаева О.А. О сущности информационных технологий // Юность и Знания - Гарантия Успеха - 2018: Сборник научных трудов 5-й Международной молодежной научной конференции. В 2-х томах, Курск, 20–21 сентября 2018 года. Курск: Университетская книга, 2018. С. 36 – 37.

[3] Системы обработки информации. Термины и определения: ГОСТ 15971-90 // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/ document/1200015664 (дата обращения: 10.06.2023).

[4] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ. URL: http://pravo.gov.ru/ (дата обращения 10.06.2022).

вредоносного ПО и распространяются хакерами через Интернет, используя альтернативные потоки[1].

Кибербезопасность – обеспечение защиты сетей, серверов, внутренних сетей и компьютерных систем, а также гарантирует, что доступ к этой информации имеют только уполномоченные лица[2].

Кибермошенничество – специальный вид мошенничества, совершенный с помощью или посредством компьютерных систем или компьютерных сетей посредством использования компьютерной информации. [3]

Киберпреследование – это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование.

Киберсквóттинг (англ. cybersquatting) – регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования. Люди, практикующие такие действия, называются киберсквóттерами.

Виды кибersквоттинга

Выделяют следующие виды занятий, обычно объединяемых термином «кибersквоттинг» или «захват доменов».

- **Тайпсквоттинг** – регистрация доменных имен, близких по написанию с адресами популярных сайтов, в расчете на ошибку части пользователей. Например, «wwwsite.example» в расчете на пользователя, который хотел попасть на «www.site.example».

---

[1] Олейникова П.А. Кейлоггеры. Вопросы санкционированного и несанкционированного применения / А.О. Свирщ // Modern Science. 2021. № 12-4. С. 289.

[2] Митряев И.С., Калимуллин Н.Р. Разграничение понятий информационной безопасности и кибербезопасности как элементов информационного пространства // Аграрное и земельное право. 2021. № 9(201). С. 159.

[3] Барчуков В.К. Терминология мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. 2017. № 4. С. 164.

• **Брендовый кибersквоттинг** – регистрация доменных имен, содержащих товарные знаки, фирменные наименования, популярные имена собственные, то есть средства индивидуализации, охраняемые законом, а также регистрация «на перспективу», например, создатель фильма «ABC» регистрирует сайт «ABC.example», а кибersквоттер, ожидая, что выйдет продолжение фильма, регистрирует на себя «ABC2.example», «ABC3.example», «ABC4.example» и т. д. При этом у кибersквоттера есть риск лишиться домена и подвергнуться ответственности, однако законные владельцы товарных знаков скорее всего предпочтут не судиться (к тому же, зачастую процесс судебного разбирательства затягивается на месяцы), а выкупить захваченные домены, и цель кибersквотера будет достигнута – он заработает на этом финансовые средства.

• **Защитный кибersквоттинг** – легальный владелец сайта (товарного знака) регистрирует все доменные имена, близкие, созвучные, похожие, связанные по смыслу с его собственным доменным именем. Делается для того, чтобы не стать жертвой кибersквоттеров. Например, владелец популярного сайта «www.firma.example» может также зарегистрировать домены «firma-msk.example» и «firma-spb.example», чтобы перенаправлять с них посетителей на свой основной сайт, а также «anti-firma.example», чтобы недоброжелатели не смогли использовать его.

• **Обратный кибersквоттинг**[1] похож на рейдерство. По закону торговая марка доминирует над доменом. Этим пользуются некоторые кибersквоттеры, находя популярный сайт без торговой марки, регистрируют имя на себя и через суд отбирают популярный сайт. Иногда владельцы идут на сделку с кибersквоттером, чтобы откупить у него торговую марку.

• **Аукционный кибersквоттинг** На таких условных аукционах идет перепродажа перспективных доменов среди самих кибersквоттеров.

Кибербуллинг – травля, оскорбления или угрозы, высказываемые жертве через социальные сети или другие средства электронных коммуникаций.

Кибер-ОПГ (организованная преступная группа), киберкриминальная структура (организация) – организация, занимающаяся преступной деятельностью в киберпространстве.

Киберпреступность, киберпреступления – литературное название преступлений, основным инструментом которых являются информационно-телекоммуникационные технологии, компьютеры и компьютерные сети. Это, например, такие традиционные преступления, как мошенничества, вымогательства (blackmail), хищения личных данных, но совершаемые через Интернет и/или с применением вычислительных устройств. Киберпреступность быстро стала серьезной мировой проблемой ввиду резкого роста числа пользователей компьютеров, смартфонов и др., и того факта, что для нее не существует никаких границ, что существенно затрудняет обнаружение и наказание киберпреступников. Отдельным видом киберпреступности является кибертерроризм.

Компьютер – (англ. computer – «вычислитель») – устройство или система устройств, способная выполнять заданную (четко определенную или изменяемую) последовательность операций на основе различных свойств (механических, электронных, биологических, оптических, квантовых и других физических явлений) компонентов ее функциональных узлов; совокупность технических средств, создающая возможность проведения обработки информации и получение результата в необходимой форме [1].

Компью́тер-зо́мби – компьютер в сети, который был заражен специализированной вредоносной программой, как правило, предоставляющей злоумышленнику удаленный доступ и ресурсы машины. Программа в большинстве случаев активно маскируется и без офлайновой проверки файлов, контроля трафика или использования специального ПО вычислить такой компьютер достаточно сложно. Такой компьютер может быть использован третьими лицами без ведома владельца: для доступа в закрытую или

[1] Системы обработки информации. Термины и определения: ГОСТ 15971-90. – Взамен ГОСТ 15971-84. // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015664 (дата обращения: 10.06.2022).

коммерческую сеть (включая Интернет), использования вычислительных ресурсов (кластеризации), рассылки спама и перенаправления трафика открытые прокси в момент совершения противоправных действий.

Компьютерный вирус − это программа или фрагмент кода, предназначенный для повреждения компьютера путем повреждения системных файлов, растраты ресурсов, уничтожения данных или других неприятностей[1].

Компьютерный терроризм (кибертерроризм) – использование компьютерных и телекоммуникационных технологий (прежде всего, Интернета) в террористических целях.

Криптовалюта – это цифровая платежная система, при проверке транзакций в которой не участвуют банки. Это система с равноправными участниками, позволяющая любому пользователю, находящемуся в любом месте, отправлять и получать платежи. Криптовалютные платежи существуют исключительно в цифровом виде в онлайн-базе данных, описывающей конкретные транзакции. Они не подразумевают операций с физическими деньгами, имеющими хождение и возможности обмена обмен в реальном мире. При переводе средств в криптовалюте, транзакции записываются в публичный реестр. Криптовалюта хранится в цифровых кошельках.

Существуют тысячи криптовалют. Ниже перечислены самые известные из них:

- **Биткойн**

Биткойн, созданный в 2009 году, стал первой криптовалютой и до сих пор сохраняет самую высокую популярность. Валюта была разработана Сатоши Накамото – считается, что это псевдоним человека или группы людей, а точная личность разработчика остается неизвестной.

[1] Гуляев В.Р., Струнькина В.А. Компьютерные вирусы — проблема XXI века // Юный ученый. 2017. № 1 (10). С. 54 – 56. URL: https://moluch.ru/young/archive/10/752/ (дата обращения: 17.06.2023).

• **Ethereum (Эфириум)**

Блокчейн-платформа Ethereum была разработана в 2015 году. Она имеет собственную криптовалюту Ether (ETH) или Ethereum. Это самая популярная криптовалюта после биткойна.

• **Litecoin**

Эта валюта больше всего похожа на биткойн, но в ней более оперативно развиваются нововведения, такие как быстрые платежи и процессы, позволяющие проводить больше транзакций.

• **Ripple**

Эта система с распределенным реестром, основанная в 2012 году. Ripple можно использовать для отслеживания различных видов транзакций, не только криптовалютных. Компания-разработчик платформы Ripple работала с различными банками и финансовыми учреждениями.

Криптовалюты, отличные от биткойна, называют общим термином «альткойны», чтобы отличать от оригинала.

Локальный интернет-регистратор (англ. Local Internet registry, LIR) – организация, занимающаяся распределением адресного пространства пользователям сетей (сервис-провайдерам и их абонентам) и оказанием сопутствующих регистрационных услуг. Как правило, локальными регистраторами управляют крупные сервис-провайдеры и корпоративные сети.

Многовекторный червь – сетевой червь, применяющий для своего распространения несколько разных механизмов (векторов атаки), например, электронную почту и эксплойт ошибки в операционной системе. В некоторых случаях черви повреждают файлы и негативно влияют на работу компьютера (если это предусмотрено создателем).

Мошенничество с платежными картами, кардинг (от англ. carding) – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно,

либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространенным методом похищения номеров платежных карт является фишинг (англ. phishing, искаженное fishing – рыбалка) – создание мошенниками сайта, который будет пользоваться доверием у пользователя, например, сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт.

Мошенничество, совершенное с помощью электронных средств платежа – хищение имущества с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой [1].

Национальный интернет-регистратор (англ. National Internet Registry, NIR) – организация под управлением регионального интернет-регистратора, занимающаяся координацией распределения IP-адресов и других интернет-ресурсов на национальном уровне в стране или экономическом блоке.

Нулевое доверие – принцип кибербезопасности, подразумевающий отсутствие изначального доверия к приложениям или пользователям, даже если они размещены в пределах организации. Вместо этого модель нулевого доверия предполагает внедрение контроля доступа с самыми минимальными привилегиями, что требует строгой аутентификации со стороны соответствующих органов и постоянного мониторинга приложений. AWS использует принципы нулевого доверия для аутентификации и проверки каждого запроса API.

Облачное шифрование засекречивает данные перед сохранением в облачных базах данных. Так, в случае утечки посторонние лица не смогут воспользоваться этими данными в злоумышленных целях. Организации используют Сервис управления

[1] Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. Москва, 2018. С. 85.

ключами AWS, чтобы контролировать шифрование данных в рабочих нагрузках AWS.

Откры́тый про́кси-се́рвер – прокси-сервер, обрабатывающий запросы от любых IP-адресов в Интернете. В отличие от обычных прокси-серверов, которыми пользуется ограниченное количество доверенных лиц (обычно в зоне ответственности владельца прокси-сервера – например, в локальной сети), открытый прокси-сервер позволяет практически любому узлу сети обращаться через себя к другим узлам сети.

Ошибочный отказ (в доступе к системе) – ложно отрицательная [аутентификация, идентификация] в ИБ – ситуация, когда зарегистрированный (легальный) пользователь пытается пройти идентификацию по биометрическим атрибутам (например, по отпечаткам пальцев), но из-за ненадежной работы средств контроля получает отказ.

Переполнение буфера – один из самых распространенных типов атак в Интернете. Принцип данной атаки построен на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа работает под учетной записью администратора системы, то данная атака позволит получить полный контроль над компьютером жертвы, поэтому рекомендуется работать под учетной записью рядового пользователя, имеющего ограниченные права на системе, а под учетной записью администратора системы выполнять только операции, требующие административные права.

Перехват – перехват данных, пересылаемых по линии связи, например содержимого незащищенных транзакций. Различают пассивный перехват – перехват без воздействия на обмен сообщениями, и активный, когда атакующий не просто контролирует обмен, но и изменяет передаваемые и/или добавляет свои сообщения.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[1].

Поведенческая аналитика позволяет отслеживать передачу данных из устройств и сетей для обнаружения подозрительной активности и аномальных действий. Например, команды по вопросам IT-безопасности получают предупреждения о резких скачках трафика во время передачи данных или о загрузке подозрительных файлов на определенные устройства.

Повышение уровня ИБ, уровня кибербезопасности (КБ), устойчивости, робастности системы в ИБ – достигается, в частности, с помощью составления, измерения, анализа и сокращения поверхности атаки и поверхности уязвимостей системы. Для ПО это выявление и удаление необязательных функций, кодов, логинов, сервисов – векторов атаки. В компьютерных системах обычно предусматривается создание многоуровневой защиты с применением средств противодействия вредоносному ПО (malware), с регулярной диагностикой средств безопасности и регулярным обновлением ПО при помощи «заплаток» от изготовителей, с удалением ненужных приложений, с физической изоляцией от небезопасных сетей и др.

Порт (англ. port) – целое неотрицательное число, записываемое в заголовках протоколов транспортного уровня сетевой модели OSI (TCP, UDP, SCTP, DCCP).

Программы-вымогатели относятся к бизнес-модели и широкому спектру смежных технологий, которые злоумышленники используют для вымогательства денег у организаций. Вне зависимости от того, делаете ли вы свои первые шаги в разработках на AWS или у вас уже есть опыт работы с ними, мы предлагаем вам специальные ресурсы, которые помогут защитить критически важные системы и конфиденциальные данные от программ-вымогателей.

Региональный интернет-регистратор (англ. Regional Internet Registry) – организация, занимающаяся вопросами адресации и маршрутизации в сети Интернет.

---

[1] О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Российская газета. 2006. 29 июля.

Существуют пять RIR:

- American Registry for Internet Numbers (ARIN) – для Северной Америки;
- RIPE Network Coordination Centre (RIPE NCC) – для Европы, Ближнего Востока и Центральной Азии;
- Asia-Pacific Network Information Centre (APNIC) – для Азии и Тихоокеанского региона;
- Latin American and Caribbean Network Information Centre (LACNIC) – для Латинской Америки и Карибского региона;
- African Network Information Centre (AfriNIC) – для Африки и региона Индийского океана.

В ходе такой разведки злоумышленник может производить сканирование портов, запросы DNS, эхо-тестирование открытых портов, наличие и защищенность прокси-серверов. В результате можно получить информацию о существующих в системе DNS-адресах, кому они принадлежат, какие сервисы на них доступны, уровень доступа к этим сервисам для внешних и внутренних пользователей.

Руткиты – это вредоносное программное обеспечение, которое попадает на зараженный компьютер и предоставляет права администратора злоумышленнику. Опасность заключается в том, что они незаметны для пользователя, операционной системы и их крайне сложно обнаружить с помощью антивирусов. К руткитам часто добавляют другой вид вредоносного ПО, так называемые клавиатурные шпионы или кейлоггеры[1].

Сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»[2].

---

[1] Олейникова П.А., Свирщ А.О. Кейлоггеры. Вопросы санкционированного и несанкционированного применения // Modern Science. 2021. № 12-4. С. 289.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

Серый список – записи в базе данных, перечисляющие все устройства, смарт-карты и иные объекты, которые находятся под подозрением в отношении безопасности.

Серый хакер – квалифицированный хакер, который берется за любую работу и занимает промежуточное положение между белыми и черными хакерами.

Сетевая безопасность обеспечивает киберзащиту для компьютеров и устройств, подключенных к сети. IT-команды используют такие технологии сетевой безопасности, как брандмауэры и управление сетевым доступом, для контроля разрешений и доступа пользователей к определенным цифровым ресурсам.

Сетевая разведка. В ходе такой атаки крэкер собственно не производит никаких деструктивных действий, но в результате он может получить закрытую информацию о построении и принципах функционирования вычислительной системы жертвы. Полученная информация может быть использована для грамотного построения предстоящей атаки и обычно производится на подготовительных этапах.

Сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.

Система высокой уязвимости в ИБ – компьютерная система, для которой как минимум один из базовых целевых показателей безопасности (конфиденциальность, целостность или готовность) имеет высокую потенциальную возможность (высокий риск) нарушения.

Система обнаружения вторжений – организации используют системы обнаружения вторжений для идентификации кибератак и быстрого реагирования на них. Современные решения для обеспечения безопасности используют машинное обучение и аналитику данных для выявления скрытых угроз в вычислительных инфраструктурах организаций. С помощью механизма защиты от вторжений, собирающего данные об инцидентах, команды по вопросам безопасности могут определять их источники.

Скимминг – частным случаем кардинга является скимминг (от англ. skim – снимать сливки), при котором используется скиммер – инструмент злоумышленника для считывания, например, магнитной дорожки платежной карты. Коммуникационные риски непосредственно связаны с общением пользователей в сети Интернет. Это понятие включает в себя незаконный контакт и киберпреследование. Незаконный контакт – это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Сниффинг пакетов – довольно распространенный вид атаки, основанный на работе сетевой карты в режиме promiscuous mode, а также monitor mode для сетей Wi-Fi. В таком режиме все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению, называемому сниффером. В результате злоумышленник может получить большое количество служебной информации: кто, откуда и куда передавал пакеты, через какие адреса эти пакеты проходили. Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

Со́кет (англ. socket – разъем) – название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой только сетью. Сокет –абстрактный объект, представляющий конечную точку соединения.

Социа́льная инженерия – в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Следует отличать от понятия социальной инженерии в социальных науках – которое не касается разглашения конфиденциальной информации. Совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного «мошенничества»

отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества[1].

Тайпсквоттинг – разновидность кибersквоттинга. Домены, имеющие схожесть с существующими брендами, но с умышленными опечатками: Ростнефть. ру; Лугойл.com; rembler.ru и т.д. Обычно хапперы не продают такие домены, а оставляют в личном пользовании для построения прибыльного бизнеса (используют сайты в качестве рекламы, на которых можно отслеживать несколько тысяч просмотров), распространения вирусов. Как правило, опечатка влечет за собой угрозу утери идентификационных данных[1]. Тайпсквоттинг – это вид атак социальной инженерии, нацеленный на пользователей интернета, допустивших опечатку при вводе веб-адреса в браузере и не использующих поисковую систему. Как правило, идея тайпсквоттинга заключается в том, чтобы обманом вынудить пользователей посетить вредоносные сайты с веб-адресами, которые являются типичным неправильным написанием адресов легальных сайтов. На этих поддельных сайтах у пользователей могут обманом запрашиваться конфиденциальные данные[2].

Теневые ИТ - это использование внутренних систем компании для выполнения задач, выходящих за их рамки или предназначение.

Например, в компании может быть принята политика, запрещающая сотрудникам использовать свои личные устройства в рабочих целях.

Однако если у сотрудника есть собственное устройство, он может получить доступ к конфиденциальной информации на этом устройстве, используя его для подключения к приложениям или документам, связанным с работой. Мы подробно рассмотрели эту тему, рассказав о том, как DMARC может помочь предотвратить теневые ИТ-практики.

---

[1] Старостенко О.А. Закономерности становления и развития кибермошенничества в России и за рубежом // Вестник Уральского юридического института МВД России. 2021. № 1(29). С. 139.

[2] Что такое тайпсквоттинг – определение и описание. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-typosquatting (дата обращения 22.06.2023).

Теневые ИТ могут представлять опасность для информационной безопасности организации, поскольку снижают контроль над доступом к данным, а также увеличивают вероятность утечки данных и нарушения безопасности.

Телефонное мошенничество (англ. vishing, от voice phishing[1]) – один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка или правоохранительных органов, покупателя и т.д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим банковским счетом / платежной картой.

Типы:

- прямое выманивание денег, когда мошенники звонят от имени родственника и просят деньги;
- шантаж, когда мошенники звонят от имени работника правоохранительных органов[5];
- банковское мошенничество, когда мошенники звонят на мобильный телефон и представляются сотрудниками банка или службы безопасности;
- звонки с требованием установить мошенническое приложение или перейти по ссылке в СМС[6].

Тро́ллинг – форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

Файл – идентифицированная совокупность экземпляров полностью описанного в конкретной программе типа данных, находящихся вне программы во внешней памяти и доступных программе посредством специальных операций[1].

[1] Организация данных в системах обработки данных. Термины и определения: ГОСТ 20886-85 // Электронный фонд правовой и нормативно-технической

Фарминг – это процедура скрытного перенаправления жертвы на ложный IP-адрес[1].

Фишинг (от англ. fishing – рыбная ловля, выуживание) – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) путем обмана или злоупотребления доверием. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, внутри социальных сетей (Facebook, ВКонтакте, Одноклассники.ru и пр.) или от имени банков (например, Ситибанк, Альфа-банк), поисковых и почтовых систем (Yandex, Mail.ru и др.)[2], Единого портала государственных услуг Российской Федерации (Госуслуги).

Хакер (от англ. to hack – разрубать) – квалифицированный IT-специалист, обладающий навыками по взлому систем защиты информации и неправомерному доступу к информационно-телекоммуникационным и иным электронным системам.

Электронная почта – корреспонденция в виде сообщений, передаваемая между пользователями через вычислительную сеть[3].

Флуд (от неверно произносимого[1] англ. flood «наводнение, поток») – малосодержательные и нетематические сообщения в интернет-форумах и чатах, зачастую занимающие большие объемы. Технический флуд представляет собой хакерскую атаку с большим количеством запросов, приводящую к отказу в обслуживании. В некоторых ситуациях флудом считается несколько сообщений подряд от одного игрового лица.

Виды флуда

документации. URL: http:// docs.cntd.ru/document/1200015708 (дата обращения 02.06.2022).

[1] Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3(17). С. 162 – 169.

[2] Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. Москва, 2018. С. 23.

[3] Судебная компьютерно-техническая экспертиза // Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/ document/1200144960 (дата обращения 26.06.2023).

- Обычный флуд сообщениями – отправка большого количества однотипных сообщений и/или однотипных/одинаковых символов/букв. Самый простой способ организовать такой вид флуда – написать некоторую фразу, а затем, используя связку Ctrl-C/Ctrl-V, отправлять ее в чат. В некоторых чатах достаточно набрать фразу и отправлять ее в чат многократным нажатием клавиши Enter, пока форма сообщения не очистится.
- Ник-флуд организуется путем ввода флудером в чат большого количества зомби-пользователей (ботов) или смены собственного ника насколько возможно часто (эффективно для IRC).
- Вайп – создание на форуме большого количества пустых тем.
- Смайл-флуд – отправка в чат сообщений, состоящих из одних смайликов или превышающих допустимое значение их количества. Например, правилами некоторых игр разрешена отправка трех маленьких смайликов или одного большого раз в три минуты.
- DoS-атака.
- Презенс-флуд – флуд статусными сообщениями (сообщениями о присутствии, «сне», «работе» – переключаемыми вручную; либо входе/выходе, сопровождающими реальные подключения/отключения с целью флуда), в основном в конференциях различных jabber-серверов.
- Микрофлуд – флуд с использованием микрофона на игровом, тим-спик или ином сервере; к микрофлуду также относится трансляция сторонней музыки на игровом сервере.

Утечка данных – одна из главных проблем ИБ, причиняет большой материальный ущерб и представляет риск других потерь. Для предотвращения этих потерь принимаются самые разнообразные способы защиты – аппаратные, программные, организационные и др. Например, average cost of a data breach – средняя стоимость утечки данных (средняя величина ущерба, потерь от инцидента утечки данных).

Эксплóйт (англ. exploit, эксплуатировать) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования (DoS-атака). Вирус для уничтожения программ, игр, приложений.

Электронная война – война с применением электронного оружия; радиоэлектронная война, радиоэлектронная борьба (РЭБ) – радиоэлектронное подавление; противодействие радиоэлектронному подавлению со стороны противника; использование электронных устройств, работающих в электромагнитном спектре, или направленной (электромагнитной) энергии для нарушения работоспособности, вывода из строя или разрушения компьютерных и телекоммуникационных систем и ВЦ противника. Электронная война может вестись пилотными и беспилотными системами вооружения с воздуха, моря, земли, космоса, причем ее целями могут быть людские ресурсы, коммуникационные системы, радиолокационные средства и/или другие виды оборудования и систем противника. Пример: Electronic warfare specialists are called “crows” because commanders referred to them by the code name “Raven” during World War II. – Специалистов по радиоэлектронной войне называют “в**о**ронами”, потому что во время Второй мировой войны командование вызывало их по кодовому слову “Ворон”.

Эти́чный ха́кер, или бе́лый ха́кер, а также на сетевом сленге бе́лая шля́па (от англ. white hat) – специалист по компьютерной безопасности, который специализируется на тестировании безопасности компьютерных систем. В отличие от черных шляп (черных хакеров), белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищенным.

Действия дежурного при получении сообщения о совершении дистанционного хищения (кибермошенничества)

1. Зарегистрировать данные заявителя:
- ФИО,
- адрес,
- номер телефона
- место работы.
2. Зарегистрировать данные потерпевшего:
- ФИО,
- адрес,
- номер телефона,
- место работы.
3. Уточнить:
- обстоятельства происшествия,
- время (период),
- место,
- способ совершения преступления, используемые средства сотовой связи (абонентских номерах), номерах расчетных счетов, банковских карт, на которые были перечислены деньги, адресе (названии) электронной почты, сайта, ID-номера страницы в сети Интернет, IP-адреса, используемого подозреваемым[1].
4. Уточнить сумму ущерба.
5. Выяснить возможных лиц, причастных к преступлению (возможность получения доступа к карте, номеру телефона и т.д.).
6. Направить на место происшествия следственно-оперативную группу (СОГ) с дополнительным привлечением необходимых специалистов.
7. Доклад руководителю территориального органа.
8. Доклад в вышестоящую дежурную часть.

[1] Об утверждении алгоритма мероприятий по раскрытию и расследованию мошенничеств, совершенных с использованием средств связи и сети Интернет: приказ МВД России от 27.11.2017 № 869.

9. По всем фактам поступивших сообщений о мошенничествах данной категории незамедлительно информирует сотрудника уголовного розыска ОВД, закрепленного приказом о создании ЛСОГ по раскрытию мошенничеств данной категории[1].

10. Установить принадлежность абонентского номера преступника к конкретному оператору сотовой компании региона Российской Федерации с использованием интернет-ресурса www.rossvyaz.ru (федеральное агентство связи (Россвязь) – выписка из реестра Российской системы и плана нумерации) с последующим внесением информации в ПК «ТОР»[2].

11. Внести в ПК «ТОР» максимально полную информацию, полученную от заявителя и в ходе проведения дополнительной проверки по заявлению и сообщению, содержащему признаки мошенничества с использованием средств сотовой связи и сети Интернет[3].

12. Получить информацию с места происшествия от руководителя СОГ.

13. Проинструктировать заявителя о мерах предосторожности и дальнейших действиях в целях сохранения следов преступления и соответствующих улик, а также минимизации негативных последствий.

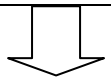
[1] Об утверждении алгоритма мероприятий по раскрытию и расследованию мошенничеств, совершенных с использованием средств связи и сети Интернет: приказ МВД России от 27.11.2017 № 869.

[2] Там же.

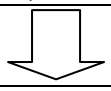
[3] Там же.

Алгоритм действий дежурного при получении сообщения о совершении дистанционного хищения (кибермошенничества)

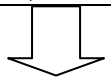
1.	Работа с заявителем



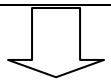
2.	Зарегистрировать данные заявителя: ФИО, адрес, номер телефона, место работы



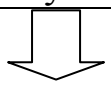
3.	Зарегистрировать данные потерпевшего: ФИО, адрес, номер телефона, место работы



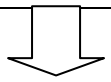
4.	Уточнить: - обстоятельства происшествия, - время (период), место, способ совершения преступления; - сумму ущерба



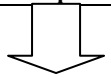
5.	Выяснить возможных лиц, причастных к преступлению (возможность получения доступа к карте, номеру телефона и т.д.)



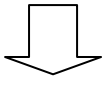
6.	Направление на место происшествия следственно-оперативную группу (СОГ) с дополнительным привлечением необходимых специалистов



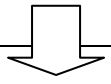
7.	Доклад руководителю территориального органа



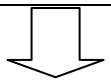
8.	Доклад в вышестоящую дежурную часть



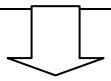
9.	Информировать сотрудника уголовного розыска ОВД, закрепленного приказом о создании ЛСОГ по раскрытию мошенничеств данной категории



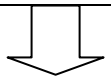
10	Установить принадлежность абонентского номера преступника к конкретному оператору сотовой компании региона Российской Федерации



11	Внести в программный комплекс «ТОР» (другие базы данных) максимально полную информацию, полученную от заявителя и в ходе проведения дополнительной проверки по заявлению и сообщению



12	Получение информации с места происшествия от руководителя СОГ



13	Проинструктировать заявителя о мерах предосторожности и дальнейших действиях в целях сохранения следов преступления и соответствующих улик

В Книге учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП) отражаются следующие сведения:

порядковый номер, присвоенный зарегистрированному заявлению (сообщению) о преступлении, об административном правонарушении, о происшествии;

дата, время и форма поступления заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о сотруднике органов внутренних дел, принявшем заявление (сообщение) о преступлении, об административном правонарушении, о происшествии;

данные о заявителе;

регистрационный номер талона-уведомления, выданного заявителю (в случае выдачи);

краткое содержание заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о руководителе, которому доложено о заявлении (сообщении) о преступлении, об административном правонарушении, о происшествии;

результаты работы следственно-оперативной группы, дежурного наряда (сотрудника) на месте совершения преступления, административного правонарушения, месте происшествия;

данные о руководителе, поручившем проверку заявления (сообщения) о преступлении, об административном правонарушении, о происшествии;

данные о сотруднике органов внутренних дел, которому поручена проверка заявления (сообщения) о преступлении, об административном правонарушении, о происшествии, его подпись, дата и время получения;

срок проверки, установленный руководителем, и срок, в который рассмотрено заявление (сообщение) о преступлении, об административном правонарушении, о происшествии, данные о должностных лицах, продливших срок проверки;

результаты рассмотрения заявления (сообщения) о преступлении, об административном правонарушении, о происшествии.

Действия потерпевшего при обнаружении несанкционированных транзакций

Как только потерпевший обнаружил в истории операций банковской карты переводы денежных средств, которые он не совершал, ему необходимо:

1. Незамедлительно заблокировать ее.

Это можно сделать при помощи интерфейса «онлайн» и опции «Заблокировать карту», а также связавшись с оператором по номерам горячей линии.

При обращении по телефону сотрудники банка спросят кодовое слово регистрируемой при получении карты. Однако в случае необходимости данную операцию они могут произвести по другим данным, например, серии, номера паспорта и т.д. Точно таким же образом в случае необходимости карту можно разблокировать.

2. Прекратить какие-либо самостоятельные манипуляции с объектами, использованными преступниками для дистанционного банковского обслуживания (ДБО) (смартфонами, телефонами, планшетами, ноутбуками, ПК, POS-терминалами, банковскими картами).

3. Если на момент поступления сообщения данный объект выключен**, включать его нельзя.**

4. Если устройство включено для недопущения удаленного подключения, направленного на совершение повторных незаконных транзакций или на удаление следов инцидента, **устройство необходимо выключить и обязательно отключить сетевые подключения, источник питания.**

5. Во избежание утраты следов инцидента **ЗАПРЕЩЕНО:**

- перезагружать устройство,
- форматировать носители,
- переустанавливать операционную систему,
- проводить проверку антивирусными программами.

6. Позвонить в полицию и сообщить о случившемся.

7. Если выяснится, что деньги с карты были переведены на счет другого банка, потерпевшему **НЕОБХОДИМО В КРАТЧАЙШИЕ СРОКИ обратиться в свой банк с заявлением на блокировку счета, на который поступили денежные средства, и последующий возврат денег.** В течение 5 дней есть большая возможность ограничить операции по банковскому счету, на который преступниками были переведены денежные средства, и через какое-то время вернуть деньги.

Типичные признаки подготовки, совершения и сокрытия дистанционного хищения (кибермошенничества)

К типичным признакам подготовки, совершения и сокрытия дистанционного хищения (кибермошенничества) относят:

- получение данных с использованием вредоносных программ, которые попадают смартфоны и дублируют вводимую информацию на сервера злоумышленников, например, при авторизации в личном кабинете своего онлайн-банка[1];

- создание «зеркальных» сайтов, которые визуально похожи на оригинал[2];

- рассылку писем или сообщений от кажущегося надежным источника с просьбой предоставить ту или иную информацию, открывающую доступ к конфиденциальным сведениям[3];

- завладение с помощью телефонного звонка ценной информацией и требование совершить определенные действия, направленные на облегчение для них хищения денежных средств[4];

- несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны компьютерных сетей (локальных; Интернет) с ослабленной политикой безопасности;

- появление в системе ПК или их сети ложных данных (письма электронной почты от неизвестных и известных адресатов с прикрепленными файлами, не соответствующими описанию, и т.п.);

- использование режима доступа пользователя сети или открытого им канала связи после завершения активной фазы работы;

---

[1] Смирнов В.М., Кузина А.В. Наиболее популярные схемы кибермошенничества в сети Интернет // Тенденции развития науки и образования. 2022. № 86-1. С. 111.

[2] Там же. С.112.

[3] Байжумаева М.А. Кибермошенничество // Новый юридический вестник. 2022. № 3 (36). С. 67 – 69. URL: https://moluch.ru/th/9/archive/224/7400/ (дата обращения: 25.06.2023).

[4] Там же.

- незаконное использование компьютерной системы или сетевых соединений за счет авторизованного абонента[1];

- нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней;

- чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию компьютерной информации определенной категории;

- создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом;

- подмена пользователя, при котором злоумышленник выдает себя за истинного владельца[2];

- введение в заблуждение, т. е. лицо, формируя правдоподобные отклики, намеренно вводит в заблуждение пользователя с целью получения некой «полезной» для него информации (например, e-mail адреса)[3].

[1] Яппаров Р.М. Оперативно-разыскная характеристика преступлений в сфере компьютерной информации // Современные проблемы уголовного процесса: пути решения: сборник материалов 2-й Международной конференции, Уфа, 8 апреля 2021 года. Уфимский ЮИ МВД России. 2021. С. 322.

[2] Там же. С. 322.

[3] Там же. С. 322.

Заключение

В эпоху всемирной цифровизации способом беспроводного доступа в информационно-телекоммуникационную сеть является Интернет, который представляет пользователю абсолютную свободу действий, а также возможность использования связи на любом устройстве – от мобильного телефона до компьютера. В настоящее время Интернет набирает высокую популярность среди всех категорий населения. Его используют не только для развлечения, общения, но и в трудовой деятельности человека. Мобильный Интернет также является главным источником информации.

В современных условиях экономической нестабильности преступность в сфере информационно-телекоммуникационных технологий приобретает новые направления, а Интернет выступает не только инструментом, но и благоприятной средой для противоправной деятельности.

Кибермошенничество – сравнительно новый феномен, представляющий собой активные действия в онлайн-формате с целью получения выгоды посредством манипуляций сознанием человека. Кибермошенничество появилось и развивается в интернет-пространстве[1].

Противодействие кибермошенничеству является одной из основных задач, должно быть комплексным и осуществляться со стороны общественности и государственного аппарата.

[1] Байжумаева М.А. Кибермошенничество // Новый юридический вестник. 2022. № 3 (36). С. 67 – 69. URL: https://moluch.ru/th/9/archive/224/7400/ (дата обращения: 25.06.2023).

Список литературы

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Уголовно-процессуальный кодекс Российской Федерации // Собрание законодательства РФ. – 2001. – № 52 (часть I). – Ст. 4921.
3. Уголовный кодекс Российской Федерации // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
4. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ // Собрание законодательства РФ. – 2011. – № 27. – Ст. 3872.
5. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3451.
6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3448.
7. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646. – СПС «КонсультантПлюс» (дата обращения 25.05.2023).
8. Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях: приказ МВД России от 29.08.2014 № 736: в ред. приказа МВД России от 07.11.2016 № 708. – СПС «КонсультантПлюс» (дата обращения 25.05.2023).

Учебная и специальная литература

1. Байжумаева М.А. Кибермошенничество / М.А. Байжумаева // Новый юридический вестник. – 2022. – № 3 (36). – С. 67 – 69. – URL: https://moluch.ru/th/9/archive/224/7400/ (дата обращения: 25.05.2023).
2. Бакаева О.А. О сущности информационных технологий / О.А. Бакаева // Юность и Знания – Гарантия Успеха – 2018: Сборник научных трудов 5-й Международной молодежной научной конференции. В 2-х томах, Курск, 20 – 21 сентября 2018 года / Ответственный редактор А.А. Горохов. – Курск: Закрытое акционерное общество «Университетская книга», 2018. – С. 36 – 39.
3. Барчуков В.К. Терминология мошенничества в сфере компьютерной информации / В.К. Барчуков // Пробелы в российском законодательстве. – 2017. – № 4. – С. 163 – 165.

4. Галактионов, Г. А. Противодействие DDOS атакам: методы и принципы защиты сайта РТУ МИРЭА / Г.А. Галактионов, В.А. Шутов // Инновации. Наука. Образование. – 2021. – № 46. – С. 772 – 777.

5. Гуляев В.Р. Компьютерные вирусы – проблема XXI века / В.Р. Гуляев, В.А. Струнькина // Юный ученый. – 2017. – № 1 (10). – С. 54 – 56. – URL: https://moluch.ru/young/archive/10/752/ (дата обращения: 17.06.2023).

6. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А.В. Аносов и др. – Москва: Академия управления МВД России, 2019. – Ч. 1. – 208 с.

7. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений / Э.Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3(17). – С. 162 – 169.

8. Кудрявцев Р.В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. – 2019. – №24 (262). – С. 218 – 221.

9. Лебедева А.А. Особенности расследования киберпреступлений // Безопасность бизнеса. – 2021. – № 6. – С. 48 – 56.

10. Матвеев Д.И. Использование товарного знака в доменном имени / Д.И. Матвеев // Проблемы правовой информатизации. – 2006. – № 2. – С. 25 − 29.

11. Митряев И.С. Разграничение понятий информационной безопасности и кибербезопасности как элементов информационного пространства / И.С. Митряев, Н.Р. Калимуллин // Аграрное и земельное право. – 2021. – № 9(201). – С. 158 – 161.

12. Олейникова П.А. Кейлоггеры. Вопросы санкционированного и несанкционированного применения / П.А. Олейникова, А.О. Свирщ // Modern Science. – 2021. – № 12-4. – С. 289 – 295.

13. Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло. – Москва: Ун-т прокуратуры Российской Федерации, 2018. – 184 с.

14. Ревенков П.В. Управление рисками в условиях электронного банкинга: автореф. дис. ... д-ра эконом. наук. Санкт-Петербург, 2013. – 43 с.

15. Семенова Т.В. Домен и доменное имя: отличия в правовом регулировании / Т.В. Семенова // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. – 2019. – № 13. – С. 120 – 127.

16. Смирнов В.М. Наиболее популярные схемы кибермошенничества в сети Интернет / В.М. Смирнов, А.В. Кузина // Тенденции развития науки и образования. – 2022. – № 86-1. – С. 110 – 113.

17. Старостенко О.А. Закономерности становления и развития кибермошенничества в России и за рубежом / О.А. Старостенко // Вестник Уральского юридического института МВД России. – 2021. – № 1(29). – С. 138 – 143.

18. Яппаров Р.М. Оперативно-разыскная характеристика преступлений в сфере компьютерной информации / Р.М. Яппаров // Современные проблемы уголовного процесса: пути решения: сборник материалов 2-й Международной конференции, Уфа, 08 апреля 2021 г. – Уфа: Уфимский ЮИ МВД России, 2021. – С. 320 – 327.

Интернет-ресурсы

1. DDoS-атаки: что это, происхождение, виды и способы защиты - https://selectel.ru/blog/ddos-attacks/ (дата обращения: 02.06.2023).

2. Вредоносное программное обеспечение. – URL: https://ru.malwarebytes.com/malware/ (дата обращения: 20.11.2022).

3. Организация данных в системах обработки данных. Термины и определения: ГОСТ 20886-85. – Взамен ГОСТ 20886-75; введ. 1986-07-01 // Электронный фонд правовой и нормативно-технической документации. URL: http:// docs.cntd.ru/document/1200015708

4. Официальный сайт Министерства внутренних дел России. – URL: https://xn--b1aew.xn--p1ai/folder/101762// (дата обращения: 10.06.2023).

5. Системы обработки информации. Термины и определения: ГОСТ 15971-90. – Взамен ГОСТ 15971-84; введ. 1992-01-01 // Электронный фонд правовой и нормативно-технической документации. – URL: http://docs.cntd.ru/ document/1200015664. (дата обращения: 10.06.2023).

6. Судебная компьютерно-техническая экспертиза. Термины и определения: ГОСТ Р 57429-2017 / введ. впервые 2017-09-01. – Электронный фонд правовой и нормативно-технической документации. – URL: http://docs.cntd.ru/ document/1200144960 (дата обращения 26.06.2023).

7. Что такое IP-адрес – определение и описание. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-an-ip-address (дата обращения 22.06.2023).

8. Что такое VPN и зачем это нужно? – URL: https://www.kaspersky.ru/blog/vpn-explained/10635/ (дата обращения: 22.06.2023).

9. Что такое тайпсквоттинг – определение и описание. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-typosquatting. (дата обращения 22.06.2023).

Учебное издание

Шмелева Ольга Геннадьевна
Лебедева Альфия Васильевна
Назмеева Лейсан Рафиковна
Минзянова Диляра Фарильевна
Хузяхметова Гузель Ильшатовна

Методические рекомендации (памятка) сотруднику дежурной части при поступлении сообщения (заявления) о совершении дистанционного хищения (кибермошенничества)

Методические рекомендации

Корректор Е.О. Смирнова
Компьютерная верстка Е.О. Смирнова
Дизайн обложки Е.В. Добрыднева
Тиражирование К.О. Фролова
Формат 60*84 1/16
Усл. печ. л. 3
Дата подписания в печать 20.09.2023
Тираж 50 экз.