УДК 004.056

И. П. Родивилин [1]

[1] *Иркутский национальный исследовательский технический университет, г. Иркутск, Российская Федерация*

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ТЕНДЕНЦИИ И ЗАЩИТА

Аннотация. В данной работе рассматриваются важные аспекты информационной безопасности в современном мире киберугроз. Особое внимание уделяется социальной инженерии как возрастающей угрозе, а также разнообразным способам атак, текущим тенденциям в этой области и роли искусственного интеллекта (ИИ) как в сфере обороны, так и в облегчении киберугроз. Важными темами также являются безопасность данных, стратегии их защиты, сохранение личной информации и влияние онлайн-платформ на киберпреступность. Учитывая постоянно меняющийся характер угроз и уязвимости, понимание этих динамик является важным элементом успеха в сфере кибербезопасности. Рассмотрена проблема функционирования ботов-пробивщиков и правовая основа их функционирования.

Ключевые слова: кибербезопасность, социальная инженерия, атаки, информационная безопасность, защита, тенденции, искусственный интеллект, безопасность данных, защита данных, личная информация, онлайн-платформы, киберпреступники.

I. P. Rodivilin [1]**,**

[1] *Irkutsk National Research Technical University, Irkutsk, Russian Federation*

SOCIAL ENGINEERING AS AN INFORMATION SECURITY THREAT: TRENDS AND PROTECTION

Abstract. This paper explores critical aspects of information security in the modern world of cyber threats. Special attention is given to social engineering as a growing threat, various attack methods, current trends in this field, and the role of artificial intelligence (AI) both in defense and mitigating cyber threats. Important topics also include data security, strategies for safeguarding data, the preservation of personal information, and the impact of online platforms on cybercrime. Given the constantly evolving nature of threats and vulnerabilities, understanding these dynamics is a crucial element of success in the field of cybersecurity.

Keywords*:* cybersecurity, social engineering, attacks, information security, defense, trends, artificial intelligence, data security, data protection, personal information, online platforms, cybercriminals.

В последние годы наблюдается стабильный рост атак на информационные системы, увеличение убытков от них, и увеличение ресурсов и времени, требуемых для выявления виновных в таких преступлениях. Эта динамика привлекает все больше внимания к вопросам информационной безопасности [10]. Эксперты сходятся во мнении, что нет перспектив на деградацию или стабилизацию данной ситуации [7]. Это подтверждается действиями на государственном уровне, в частности принятие указа о создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и утверждение новой доктрины информационной безопасности [8].

Большинство современных исследований в области информационной безопасности [1,3,4] сосредотачивается на улучшении технических аспектов безопасности и к разработке методов и средств, которые уменьшают вероятность успешных атак. Однако сами пользователи информационных систем остаются одними из самых уязвимых точек в систем информационной безопасности и социальная инженерия стала популярным методом атак на информационные системы [11].

Персональные и корпоративные данные стали новой валютой XXI века. В связи с этим социальная инженерия становится все более актуальной, и ее масштаб увеличивается с каждым годом. Факторы, такие как пандемия, удаленная работа и повышенные уровни стресса, способствуют увеличению инвестиций злоумышленников во вредоносные схемы и мошеннические программы.

Несмотря на использование самых современных технических средств в области информационной безопасности, человеческий фактор остается слабым звеном. По статистике, 80% успешных атак на банки в РФ в последние три года начались с применения социальной инженерии. С развитием технологий искусственного интеллекта, deepfake и атак «как сервис», применение социальной инженерии только усилится.

Обычно социальная инженерия применяется на ранних этапах атаки или для сбора информации о цели атаки. Однако стоит учитывать разнообразные виды фишинга, такие как направленные атаки на ключевых лиц (whaling) или компрометация деловой почты (BEC - Business Email Compromise), которые изначально ориентированы на корпоративный сектор и целятся в монетизацию усилий злоумышленников. В случае успешной атаки, последствия могут быть значительными, включая потерю чувствительной информации для организации и финансовый ущерб.

Один из распространенных методов социальной инженерии – это вишинг, который включает использование голосового общения для манипуляции жертвами. Этот метод может осуществляться через телефонные звонки с использованием автоматических голосовых сообщений или подделкой человеческого голоса.

Злоумышленники также могут использовать метод «Услуга за услугу», предлагая услуги или предметы взамен на конфиденциальную информацию или доступ к системам. Этот метод может использоваться для манипуляции жертвами, создавая взаимовыгодные отношения.

Актуальность вопросов защиты от социальной инженерии и оценки уровня защищенности пользователей и персонала подчеркивается инцидентами, такими как взлом почты директора ЦРУ [2], утечка секретных файлов, связанных с Эдвардом Сноуденом [6].

Эти инциденты подчеркивают, что атаки, происходящие из-за человеческого фактора, могут иметь серьезные последствия и требуют особого внимания в области информационной безопасности. Особое внимание следует уделить веб-атакам, которые могут быть разделены на следующие категории:

- Аутентификация, включает атаки, направленные на идентификацию пользователей, такие как метод «Грубая сила» для подбора паролей, недостаточная аутентификация, и слабая проверка восстановления пароля.

- Авторизация. Это класс атак, нацеленных на повышение уровня прав доступа пользователя на сайте, включая предсказание учетных данных/сессий, недостаточное завершение сессии и фиксацию сессии.

- Атаки на стороне клиента, то есть такие атаки, как подмена содержания страницы (Content Spoofing) и межсайтовое выполнение сценариев (Cross-site Scripting или XSS).

- Выполнение команд. Это метод взлома, при котором злоумышленник внедряет вредоносные команды в уязвимую систему с целью злоупотребления данными на сервере. Когда злоумышленник обнаруживает уязвимость, он может внедрить команды в любое уязвимое поле или параметр, где ввод пользователя недостаточно фильтруется. Например, это может быть поле ввода на веб-сайте, где пользователь может вводить команды. Когда сервер получает такой пользовательский ввод, он выполняет команду без должной проверки. Злоумышленник может использовать эту уязвимость для выполнения различных действий на сервере, таких как чтение, запись или удаление файлов, выполнение произвольных команд операционной системы и даже получение полного контроля над сервером.

Дополнительная атака на программу заставляет ее выполнить непредвиденную команду. Рассмотрим ситуацию, когда программа должна продублировать указанный пользователем файл, присвоив ему другое имя, возможно, чтобы создать резервную копию. Если программисту не хочется писать много кода, он может воспользоваться системной функцией, которая запускает оболочку и выполняет переданные ей аргументы как команду оболочки.

Для примера, в языке C можно воспользоваться функцией system("ls >file-list"), которая запускает оболочку и создает список всех файлов в текущем каталоге, записывая его в файл

под названием file-list. Программа запрашивает у пользователя имена файла-источника и файла-назначения, затем создает командную строку, использующую команду cp, и выполняет ее с помощью функции system.

Однако, увы, такой подход открывает уязвимость в системе безопасности, известную как внедрение команд (command injection). Предположим, что вместо ввода "abc" и "xyz" пользователь вводит «abc» и «xyz; rm -rf /». Теперь программа создает и выполняет следующую команду: cp abc xyz; rm -rf /, которая сначала копирует файл, а затем пытается рекурсивно удалить каждый файл и каталог во всей файловой системе. Если программа выполняется с привилегиями суперпользователя, эта атака может быть успешной. Проблема заключается в том, что все, что идет после точки с запятой, интерпретируется как команда оболочки. Поэтому важно учесть этот тип угрозы и принимать соответствующие меры безопасности при написании программного обеспечения.

- Логические атаки. Раскрытие информации лицам, доступ к которым им запрещен, либо раскрытие информации в результате неверной настройки веб-приложения или веб-сервера. Логические атаки направлены на эксплуатацию функций приложения или логики его функционирования.

- Телефонный фрикинг. Этот метод включает в себя взлом телефонных систем путем подбора различных кодов. Тоновый набор, использованный в корпорации Bell в США, предоставлял возможность передавать служебные сигналы. Социоинженеры пытались имитировать эти сигналы, чтобы осуществлять бесплатные звонки и даже получать доступ к администрированию телефонной сети.

И особое внимание следует уделить такому виду социоинженерной атаки как «сбор информации из открытых источников». Злоумышленники могут использовать информацию, доступную в открытых источниках, таких как социальные сети и веб-сайты компаний, для целенаправленной атаки.

Для атаки данного вида, злоумышленники используют «Боты-пробивщики» – это системы, которые собирают информацию о гражданах из разных баз данных, полученных в основном нелегальным путем через утечки данных из организаций и государственных учреждений. Такие действия формально нарушают закон, и должны привлечь к ответственности как тех, кто украл такие данные, так и тех, кто использует их незаконно. Люди, использующие «ботов-пробивщиков», должны рассматриваться как операторы персональных данных и соответственно соблюдать все требования законодательства в этой области.

Использование ботов-пробивщиков в России наказывается административной ответственностью с небольшими штрафами. Однако на практике, привлечение владельцев таких ботов затруднено, так как установление их личности и физическое присутствие за пределами России являются сложными процессами. Увеличение ответственности не решит проблему утечек баз данных, а также не обеспечит неотвратимости наказания.

Ранее, несколько популярных ботов были заблокированы администрацией Telegram, которые позволяли получать информацию о любом человеке по запросу [1].

Персональные данные или личная информация – это информация, которая относится к конкретному физическому лицу, которое можно идентифицировать по этой информации, даже если это не упоминается напрямую. Эта информация может быть разглашена другим лицам. С развитием сетей связи и автоматизации анализа данных, централизованное сбор информации о человеке стало более распространенным, а некоторые люди даже могут получать эту информацию незаконно. Эта информация может быть использована для выслеживания человека, планирования преступления, мошенничества или даже для более мирных целей, таких как реклама. Несмотря на то, что это юридический термин, современные технологии позволяют идентифицировать людей по косвенным признакам.

Кроме того, в статье 137 УК РФ закреплены уголовные нормы за незаконный сбор или распространение сведений о частной жизни лица без его согласия. Это включает в себя как личные, так и семейные тайны, которые могут быть разглашены в публичных выступлениях,

в произведениях, представленных публично, в средствах массовой информации, а также при использовании служебного положения.

С учетом развития технологий и широкого использования мобильных приложений, социальных сетей и устройств интернета вещей, особенно важно, чтобы пользователи были внимательны к разрешениям на доступ к конфиденциальной информации. Это необходимо для соблюдения всех требований закона и стандартов, касающихся защиты корпоративных данных. Ответственное отношение к обработке персональных данных является ключевым элементом обеспечения безопасности и конфиденциальности граждан в современном цифровом мире.

Настройка пользовательского доступа не является гарантией защиты персональных данных в социальных сетях. Например, пользователь может быть неосторожным и случайно разрешить доступ к своим данным ненадежному приложению или сервису, что может привести к утечке его персональных данных. Кроме того, даже если пользователь настроил доступ к своим данным только для своих друзей, его друзья могут переслать или скопировать эти данные и передать их третьим лицам, не имеющим прав на доступ к этим данным.

Кроме того, пользователь может сознательно или неосознанно размещать в социальных сетях данные, которые могут быть использованы для его идентификации или нарушения его конфиденциальности. Например, пользователь может разместить фотографию своего паспорта или другого документа, содержащего персональные данные.

Однако, как вы сказали, пользователи всегда могут обратиться к оператору персональных данных с запросом на исключение своих данных из обработки. Это право гарантировано законодательством РФ, и его соблюдение обязательно для всех операторов персональных данных. Также, для защиты персональных данных, пользователи могут использовать специальные программы и инструменты, которые помогают обезличивать данные или скрывать их от сторонних сервисов и приложений.

Данные, предоставляемые через открытые API и стандарты открытых данных, могут использоваться для персонализации веб-страниц и других интернет-приложений. Они могут использоваться для создания персонализированных рекомендаций, предложений и рекламы для пользователей. В то же время, важно учитывать права и интересы пользователей в отношении их персональных данных, чтобы обеспечить соответствие законодательству о защите персональных данных и предотвратить возможные нарушения и злоупотребления.

В то же время, киберпреступники будут все более изобретательными и хитрыми в использовании своих техник. Это происходит потому, что среди людей растет осведомленность о кибератаках, и они становятся более бдительными при получении сообщений от незнакомых отправителей. Также они обращают внимание на подозрительное поведение в онлайн-среде.

Информационные системы предприятий становятся все более надежными, поэтому для мошенников часто проще обмануть человека. Они постоянно разрабатывают новые и все более изощренные методы "социальных афер" и уделяют особое внимание психологическим аспектам, таким как любопытство, уважение к властям, желание помочь другу и доверчивость. Эти методы позволяют им продолжать проникать в систему мышления и находить уязвимости для кражи персональной информации.

Социальная инженерия представляет серьезную угрозу для предприятий и может повлечь за собой ряд негативных последствий для бизнеса. Злоумышленники могут осуществить доступ к конфиденциальной информации, украсть интеллектуальную собственность или скомпрометировать системы безопасности. Это может привести к серьезным финансовым убыткам, повреждению репутации компании и юридическим последствиям. Атаки социальной инженерии также могут вызвать нарушение бизнес-процессов и снижение производительности и компаниям могут потребоваться значительные ресурсы для восстановления систем, данных и устранения выявленных уязвимостей, что часто является дорогостоящим и трудоемким процессом.

Для противодействия атакам социальной инженерии существует множество инструментов и методов. Эффективными средствами защиты являются многофакторная аутентификация, регулярное обновление программного обеспечения, управление доступом к информации и ресурсам, регулярные резервные копии данных, а также шифрование конфиденциальных данных и непрерывный мониторинг систем безопасности и сетевой активности.

Что касается выявления и реагирования на угрозы, на российском рынке существует разнообразие решений, включая SIEM (системы управления информационной безопасностью и событиями) и MDR/MXDR (услуги мониторинга и реагирования на инциденты). Основное здесь - определить необходимое время для выявления и реагирования на угрозы. Например, если среднее время, через которое сотрудник открывает электронное письмо, составляет 25 минут, то системы безопасности должны способны быстро обнаруживать и реагировать на угрозы в этом временном окне, чтобы обеспечивать эффективную защиту.

Почему, несмотря на проведенное обучение и информирование, пользователи все равно доверяют социальным инженерам? Евгений Верезуб указывает на несколько причин, объясняющих, почему даже опытные и информированные пользователи могут стать жертвами атак. Во-первых, злоумышленники постоянно совершенствуют свои методы, что делает их атаки более изощренными и трудно выявляемыми. Во-вторых, люди часто доверчивы и эмоциональны, что делает их уязвимыми перед атаками социальной инженерии. Доверие - важный аспект межличностных отношений, и многие склонны верить другим, особенно если они кажутся надежными. Также эмоции могут оказывать влияние на принятие решений и поведение человека. В-третьих, некоторые пользователи могут не следовать рекомендациям по информационной безопасности и не принимать меры по защите своих систем, что часто приводит к компрометации их данных и систем.

Цифровая гигиена должна стать привычкой в наше время, а не исключением. В мире полной открытости в Интернете, пользователи должны быть более осторожными и бдительными в отношении своих личных данных и информационной безопасности.

Атаки социальной инженерии могут успешно проводиться из-за таких факторов, как срочность и страх. Они могут использовать эмоциональные воздействия, такие как страх перед утерей учетных данных или неотложная потребность в действиях. Помимо этого, социальные инженеры могут использовать изощренные тактики, такие как создание поддельных веб-сайтов или использование личной информации цели для получения доверия.

Чтобы успешно провести атаку социальной инженерии, злоумышленникам необходимо вызвать эмоции у жертвы и заставить ее отключить рациональное мышление. Это может достигаться с помощью разных методов, таких как поддельные истории, создание убедительных персонажей или манипуляция с эмоциями. Такие атаки могут быть сложно выявляемыми, так как они могут быть идентичными реальному взаимодействию пользователя с другими людьми или организациями.

Технические средства защиты от социальной инженерии представляют собой комплекс различных программных и аппаратных решений, разработанных для предотвращения и обнаружения атак, основанных на манипуляциях с человеческим фактором. Эти средства предназначены для защиты от мошеннических действий, которые могут включать в себя обман, манипуляцию, внушение, подкуп и другие формы воздействия на человеческое поведение с целью получения несанкционированного доступа к конфиденциальной информации или выполнения вредоносных действий в системе.

Одним из основных технических средств защиты являются системы фильтрации электронной почты. Они осуществляют проверку входящих сообщений на наличие подозрительных ссылок, вирусов и вредоносных вложений. Антивирусные программы способны обнаруживать и блокировать вредоносные коды, в том числе те, которые могут быть использованы социальными инженерами.

Системы мониторинга активности пользователей предоставляют возможность отслеживать поведение сотрудников в сети и выявлять аномалии, которые могут быть связаны

с атаками социальной инженерии. Такие системы могут автоматически сигнализировать о подозрительных действиях, например, если кто-то пытается получить доступ к конфиденциальным данным или изменить настройки без необходимых прав доступа.

Системы многофакторной аутентификации (MFA) являются одним из наиболее эффективных средств защиты. Они требуют от пользователей предоставить два или более подтверждающих фактора, таких как пароль, отпечаток пальца, SMS-код, смарт-карта или биометрические данные, чтобы получить доступ к системе. Это делает взлом учетных записей сложнее, даже если злоумышленники получили пароль.

Системы предотвращения утечек данных (DLP) мониторят и контролируют передачу конфиденциальной информации внутри и вне организации. Они могут блокировать или предупреждать о попытках передачи конфиденциальных данных, что может помочь предотвратить утечки информации из-за атак социальной инженерии.

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) также могут быть использованы для борьбы с атаками социальной инженерии. Они способны обнаруживать подозрительную активность в сети и автоматически реагировать, блокируя потенциально вредоносные соединения или действия.

Использование систем машинного обучения и искусственного интеллекта также становится все более распространенным для обнаружения аномалий в поведении пользователей и автоматического реагирования на подозрительные события.

Примером системы мониторинга активности пользователей может служить система User Activity Monitoring (UAM). Эта система предоставляет возможность организациям отслеживать и анализировать активности пользователей внутри компьютерных сетей и на рабочих станциях. UAM позволяет учитывать следующие параметры:

Мониторинг доступа к файлам и папкам. Система отслеживает, кто, когда и какие файлы открывает, изменяет, удаляет или копирует. Это позволяет выявить несанкционированный доступ к конфиденциальным данным.

Мониторинг активности в интернете. UAM фиксирует посещенные веб-сайты, время пребывания на них и активность пользователя в интернете. Это может помочь выявить использование вредоносных или нежелательных веб-ресурсов.

Мониторинг активности в приложениях. Система отслеживает, какие приложения запущены на компьютере пользователя, какие действия в них совершаются и какие данные вводятся. Это позволяет выявить подозрительные или некорректные действия в приложениях.

Мониторинг электронной почты. UAM может анализировать электронные сообщения, включая вложения и ссылки. Это позволяет выявить попытки фишинга или передачу конфиденциальных данных через электронную почту.

Мониторинг активности на серверах. Система отслеживает запросы к серверам, действия пользователей на серверах и доступ к серверным ресурсам. Это помогает обнаруживать несанкционированные попытки доступа к серверам.

Создание журналов и алертов: UAM генерирует журналы активности и автоматические оповещения (алерты) при обнаружении подозрительных действий. Алерты могут быть связаны с необычными попытками доступа, использованием неправомерных прав или другими подозрительными событиями.

Существуют российские аналоги системы мониторинга активности пользователей, подобные User Activity Monitoring (UAM). Эти системы разработаны с учетом законодательства и требований Российской Федерации к безопасности информации. Они предоставляют схожие функции, включая мониторинг активности пользователей, контроль доступа к ресурсам, анализ сетевой активности и обнаружение аномалий:

SystemWatchdog. Российское решение, предоставляющее возможности мониторинга активности пользователей в реальном времени, анализа событий и генерации отчетов о действиях пользователей в сети и на компьютерах.

NetTracker. Система разработана в России и предоставляет возможности отслеживания активности пользователей в корпоративной сети, включая мониторинг интернет-серфинга, посещенных веб-сайтов и активности в приложениях.

UserGate UAM. Российское решение, предоставляющее функции мониторинга активности пользователей, фильтрации веб-сайтов и контроля приложений в корпоративной сети.

В современном информационном мире атаки социальной инженерии представляют собой серьезную угрозу для безопасности данных и конфиденциальности. Для эффективного противодействия этому виду угрозы необходим комплексный и эшелонированный подход.

Одним из ключевых методов защиты от атак социальной инженерии является внедрение многофакторной аутентификации, что позволяет дополнительно обеспечить безопасность доступа к системам и данным. Регулярное обновление программного обеспечения, управление доступом и регулярные резервные копии данных также играют важную роль в обеспечении безопасности информации. Применение шифрования конфиденциальных данных и непрерывный мониторинг систем безопасности и сетевой активности также являются неотъемлемой частью комплексного подхода к защите от атак социальной инженерии.

Ключевым аспектом борьбы с социальной инженерией является построение инфраструктуры в соответствии с концепцией Zero Trust. Этот подход предполагает, что пользователи уже могли быть скомпрометированы, и поэтому предполагает микросегментацию сети и ограничение доступа сотрудников минимальными привилегиями. Эффективная защита также включает в себя защиту сетевой почты от спама и фишинга, использование антивирусных решений на сетевом и хостовом уровнях, а также применение "песочниц" для обнаружения неизвестных угроз.

В современных системах безопасности значительную роль играет искусственный интеллект. Использование ИИ позволяет анализировать тексты и выявлять аномалии в них, а также анализировать содержание и атрибуты коммуникации для обнаружения потенциальных угроз. ИИ также может выявлять аномалии в поведении пользователей, что может свидетельствовать о компрометации учетных записей. Технологии ИИ также могут использоваться для мониторинга активности в социальных сетях и выявления deepfake технологий.

Несмотря на проведенное обучение и информирование, пользователи всё равно могут стать жертвами атак социальной инженерии. Это объясняется тем, что злоумышленники постоянно совершенствуют свои методы, делая атаки более изощренными и трудно выявляемыми. Люди, в свою очередь, часто доверчивы и эмоциональны, что делает их уязвимыми перед атаками социальной инженерии. Доверие и эмоции играют ключевую роль в межличностных отношениях, что делает людей склонными к вере в других. Некоторые пользователи также могут не следовать рекомендациям по информационной безопасности и не принимать меры по защите своих систем, что приводит к компрометации их данных и систем.

Для эффективной борьбы с атаками социальной инженерии важно, чтобы цифровая гигиена стала привычкой. В мире полной открытости в Интернете пользователи должны быть более осторожными и бдительными в отношении своих личных данных и информационной безопасности.

С учетом тенденций развития угроз в сфере социальной инженерии, автоматизация массовых атак и персонализированные атаки становятся все более распространенными. Автоматизированные атаки могут использовать украденную и публичную информацию для повышения успешности атаки, в то время как персонализированные атаки направлены на ключевых руководителей и администраторов систем. Развитие новых технологий, таких как голосовые deepfake и социальное майнинг, создает дополнительные вызовы для специалистов по информационной безопасности в борьбе с этими угрозами.

В заключение, для эффективной борьбы с атаками социальной инженерии необходимо постоянное обновление технических средств защиты, обучение и информирование

пользователей, а также применение современных технологий, включая искусственный интеллект, для выявления и предотвращения потенциальных угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Азаров, А.А. Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищённости персонала информационных систем от социоинженерных атак: дис. канд.тех.нук: 05.13.19 / Азаров Артур Александрович. — СПб., 2013. — 232 с.
2. Американский школьник признался во взломе почты директора ЦРУ [Электронный ресурс]. Режим доступа: https://www.rbc.ru/rbcfreenews/56258e3d9a794770226404d4 (дата обращения: 30.09.2023).
3. Берова Д.М. Кибератаки как угроза информационной безопасности // Пробелы в российском законодательстве. 2018. №2. URL: https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti (дата обращения: 30.09.2023).
4. Борисова Е.С., Белоусов А.Л. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Russian Journal of Economics and Law. 2019. №3. URL: https://cyberleninka.ru/article/n/innovatsii-kak-instrument-obespecheniya-informatsionnoi-bezopasnosti-i-povysheniya-effektivnosti-deyatelnosti-bankovskoi-sistemy (дата обращения: 30.09.2023).
5. Веснина С.Н., Неустроева А.В., Степанюгин К.В. Модификация киберугроз в условиях сложной эпидемиологической обстановки, вызванной распространением вируса «Cocid-19» // Гуманитарные, социально-экономические и общественные науки. 2020. №9. URL: https://cyberleninka.ru/article/n/modifikatsiya-kiberugroz-v-usloviyah-slozhnoy-epidemiologicheskoy-obstanovki-vyzvannoy-rasprostraneniem-virusa-covid-19 (дата обращения: 30.09.2023).
6. Пентагон подсчитал, что Э.Сноуден похитил 1,7 млн секретных файлов [Электронный ресурс]. Режим доступа: https://www.rbc.ru/politics/10/01/2014/570415b79a794761c0ce5807 (дата обращения: 30.09.2023).
7. Угрозы кибербезопасности для малого и среднего бизнеса [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5999865.
8. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс]. 2016. Российская Газета. Режим доступа: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html.
9. Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс]. Российская Газета. 2013. Режим доступа: http://www.rg.ru/2013/01/18/kompataki-site-dok.html.
10. Число кибератак в России и в мире [Электронный ресурс]. Режим доступа: https://www.tadviser.ru.
11. Янгаева М.О. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СПОСОБ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ // Вестник Сибирского юридического института МВД России. 2021. №1 (42). URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-sposob-sovershenia-kiberprestupleniy (дата обращения: 30.09.2023).

REFERENCES

Информация об авторе

Родивилин Иван Петрович – к. ю. н., доцент центр компетенций по кибербезопасности, Иркутский национальный исследовательский технический университет, г. Иркутск, e-mail: 377a@bk.ru

Authors

Ivan Petrovich Rodivilin - Candidate of Law, Associate Professor, Competence Center for Cybersecurity, Irkutsk National Research Technical University, Irkutsk, email: 377a@bk.ru

Для цитирования

Родивилин И.П. социальная инженерия как угроза информационной безопасности: тенденции и защита // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №4. – С. 12-24 – Режим доступа: http://ismm-irgups.ru/toma/12-2019, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 25.02.2019)

For citations

Rodivilin I.P. Social Engineering as a Threat to Information Security: Trends and Protection // "Information Technology and Mathematical Modeling in the Management of Complex Systems": electronic scientific journal. – 2023. – No.4. – P. 12-24. – Access mode: http://ismm-irgups.ru/toma/12-2019, free access. – Title from the screen. – Language: Russian, English. (Accessed: 25.02.2019)