Инженерный вестник Дона, №3 (2023)
ivdon.ru/ru/magazine/archive/n3y2023/8259

Преимущества и недостатки использования личных мобильных устройств в финансовых организациях

Г.В. Терещенко, Ю.А. Новикова, Д.А. Попов

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В этой статье рассматриваются уязвимости информационных систем, связанные с использованием личных мобильных устройств в компаниях, предоставляющих финансовые услуги. Рекомендации этого исследования помогут осознать важность формулирования политики информационной безопасности в данной ситуации. Использование личных устройств сотрудниками стало распространенным на рабочем месте из-за возросшей зависимости бизнес-процессов от сервисов, расположенных в сети Интернета, и достижений в области технологий. Организации выгодно то, что сотрудники покупают, используют собственные устройства, таким образом, организация снижает расходы на обеспечение рабочих мест сотрудников компьютерным оборудованием и программным обеспечением. Однако компания может понести огромные убытки, если использование и подключение личных устройств к инфраструктуре информационных технологий компании не регулируется и не контролируется. Взлом личных устройств злоумышленниками позволяет получить несанкционированный доступ к активам информационных систем. Финансовые учреждения обрабатывают строго конфиденциальную информацию, что делает их более уязвимыми в случае использования личных устройств. Был проведен метод качественного исследования со специально отобранными участниками, работающими в отделах информационной безопасности финансовых учреждений. Исследование выявило отсутствие политики информационной безопасности, касающейся личных устройств и использование сотрудниками неограниченного количества таких устройств.
Ключевые слова: личные мобильные устройства, информационная безопасность, несанкционированный доступ, уязвимости, кибератака.

Введение

В настоящее время становится все более распространенным использование в информационных системах организаций концепции «Принеси своё собственное устройство» (Bring your own device - BYOD). BYOD - это концепция, относящаяся к разрешению использования личных мобильных устройств, таких как ноутбуки, планшеты и смартфоны, для доступа к сетям, системам и конфиденциальной информации компании в организации. BYOD-устройства стали преобладать на рабочем месте из-за растущей зависимости от Интернета и достижений в области технологий. Данные устройства используются для работы с электронной почтой,

голосовой связи и видеоконференций, доступа к календарям и контактной информации на работе. А такие приложения, как офисные пакеты и инструменты повышения производительности, позволяют им эффективно выполнять задачи, традиционно выполняемые на настольном компьютере. BYOD предлагает сотрудникам компаний удобство использования собственных устройств, большую простоту использования и позволяет настраивать устройства в соответствии с индивидуальными потребностями. Всякий раз, когда персональные устройства взаимодействуют с корпоративной сетью, существует риск потери и взлома данных, и, к сожалению, потенциальные риски безопасности, связанные с конфиденциальностью, остаются незамеченными для многих организаций, что создает проблемы безопасности для информационных систем ИС. Безопасность ИС включает в себя защиту информации и ИС от несанкционированного доступа (НСД). Это означает, что использование BYOD в неконтролируемых средах увеличивает уязвимость информации и ИС компании. Финансовые учреждения обрабатывают конфиденциальную информацию, что делает их мишенью для кражи данных. Поэтому внедрение BYOD в таких компаниях более опасно.

Риски, связанные с нарушениями безопасности, могут оказать неблагоприятное воздействие на финансовые учреждения, что может нанести ущерб их репутации, прибыльности и даже привести к закрытию бизнеса. Тридцать процентов всех атак вредоносного программного обеспечения (ПО) в 2020 году были нацелены на финансовые учреждения [1]. Критической проблемой BYOD является осуществление контроля доступа с устройств к данным организации [2]. Поэтому, при применении политики безопасности BYOD, следует учитывать такие аспекты, как контроль доступа, обнаружение вторжений, криптография, безопасность устройств и управление безопасностью [3]. Важно понимать, как концепция BYOD может

негативно повлиять на стратегию безопасности информационных систем компании. Согласование BYOD с политиками информационной безопасности (ИБ) компании помогает руководителям определить, что разрешено делать сотруднику при доступе к корпоративной сети. Важно иметь внутренний документ компании, в котором содержится информация для сотрудников об их обязательствах в отношении информационных активов фирмы. Таким документом может быть политика безопасности (ПБ). ПБ могут содержать рекомендации для BYOD, но при этом не включать технические рекомендации, которым могут следовать сотрудники, что приводит к тому, что сотрудники недооценивают кибер-риск, которому подвержены их мобильные устройства, и поэтому не рассматривают мобильные атаки как реальную угрозу [4].

Инсайдерские атаки и случайная публикация конфиденциальной информации сотрудниками имеют наибольшее влияние на безопасность, уступая хакерским атакам в успешном взломе их организаций [5]. Компании беспокоятся о поддержании безопасности, а сотрудники озабочены сохранением удобства работы на своих мобильных устройствах и конфиденциальностью своей личной информации.

Проблемы, возникающие в связи с соблюдением политики безопасности, заключаются в том, что сотрудники могут чувствовать, что существуют препятствия для использования их устройств, например, они не знакомы с установленным программным обеспечением безопасности, которое может ограничить доступ к их устройству.

Отсутствие надлежащей защиты и увеличение количества BYOD-устройств в организациях еще больше затрудняют обнаружение и предотвращение утечки информации [6].

Анализ угроз ИБ, связанных с внедрением BYOD

Хотя концепция BYOD обеспечивает преимущества для сотрудников и бизнеса, она также создаёт множество проблем для организаций. BYOD-устройства подключаются к точкам доступа к беспроводной сети на рабочем месте, что делает организации уязвимыми для потенциальных атак, проникающих через устройства. Поскольку устройства находятся в частной собственности, перед ИТ стоит задача по защите своих информационных активов и конфиденциальные данные от взлома, потери или неправомерного использования.

Угроза ИБ: Скомпрометированные данные. Безопасность данных ставится под угрозу, когда устройства потеряны или украдены. По данным [7], все больше устройств, которые были утеряны или украдены, содержимое которых просматривалось кем-то, кроме их владельцев. Поскольку BYOD могут содержать конфиденциальные данные компании, они открывают доступ к этой информации нарушителям ИБ.

Угроза ИБ: Атаки вредоносных программ. Компании все чаще подвергаются воздействию вредоносных программ, созданных с целью повреждения устройств, кражи информации и даже для управления устройствами. Вредоносные программы могут быть закодированы в приложения, установленные на устройствах, или обнаружены при посещении пользователем взломанного веб-сайта.

Ярким примером такого ПО является Carbanak. Carbanak – относится к компьютерным червям. Целью данного вредоносного ПО является компьютерное оборудование банковских учреждений, работающее под управлением семейства операционных систем Microsoft Windows.

Основной целью кибер-атаки является вывод денег из банка. Вывод денежных средств осуществляются через банкоматы или онлайн-банкинг. На

первом этапе через сервис электронной почты атакуются персональные компьютеры рядовых сотрудников банка.

На втором этапе производится сбор информации о том, как устроена работа в этом банке, и кто за что отвечает. Также нарушители ИБ захватывают контроль над компьютерами системных администраторов и руководителей разных уровней.

На третьем этапе производится вывод денег разными способами, с учетом специфики работы ИС конкретного банка.

Carbanak обнаружила компания «Лаборатория Касперского» в 2014 году во время совместного расследования с Европолом и Интерполом. Данное вредоносное ПО получило название по имени группы хакеров применявшего его [8].

Угроза ИБ: Злонамеренные инсайдеры. Злоумышленники-инсайдеры злоупотребляют своими высокими привилегиями и знаниями об организации для доступа к конфиденциальным данным, информации и другим ценным активам в своих корыстных целях. Из-за характера BYOD это стало еще большим риском ввиду технических возможностей устройства [9].

Угроза ИБ: Теневые информационно-технологические (ИТ) ресурсы. BYOD привел к использованию теневых ИТ ресурсов, использованию связанных с ИТ облачных сервисов, оборудования или приложений без ведома отдела ИТ или службы безопасности организации. Рост теневых ИТ во многом связан с желанием сотрудников работать более эффективно и обойти недостатки информационных систем, развернутых в организациях [10]. Только 60% ИТ-менеджеров признают теневые ИТ существующим явлением в своей организации, поскольку сотрудники и бизнес используют эти ИТ-ресурсы автономно для поддержки своих процессов [11]. Теневые ИТ затрудняют для ИТ-отделов отслеживание, управление, обслуживание и защиту ИТ-инфраструктуры на рабочем месте, поскольку организация не

знает об устройствах, подключенных к их сетям. В тех случаях, когда данная информация собирается, не всегда принимаются полноценные меры по обеспечению ИБ. Большинству организаций не удается решить проблемы безопасности с помощью формальных политик и создания средств контроля, чтобы свести к минимуму их возникновение [12].

Угроза ИБ: Отсутствие политик BYOD. Управление личными устройствами сотрудников - задача непростая и, к сожалению, не должным образом реализуется в большинстве организаций [13]. Большинству организаций не удается решить проблемы безопасности с помощью формальных политик и создания средств контроля, чтобы свести к минимуму их возникновение. Отсутствие политики BYOD означает, что сотрудники не обучены тому, как ответственно и эффективно использовать личные технологии для работы, что помогло бы вообще избежать многих проблем с безопасностью [14]. Для организаций становится постоянной проблемой отслеживать и обновлять политики BYOD, поскольку технологии и законодательные законы, касающиеся уровня контроля организаций, постоянно развиваются. Многие организации внедряют политики безопасности для предотвращения угроз безопасности BYOD, но сотрудники часто игнорируют их. Другие проблемы, которые возникают сами по себе, заключаются в том, что сотрудники не знают о существующих политиках BYOD или забывают, что политики BYOD были им представлены. Учитывая постоянные случаи промышленного шпионажа и утечки информации внутри организаций, очевидно, что необходимо строгое соблюдение политики BYOD.

Если политика не выполняется, то она теряет свою эффективность. Хотя многие организации внедряют политики безопасности для предотвращения угроз безопасности BYOD, сотрудники часто игнорируют их [15]. Другие проблемы, которые возникают сами по себе, заключаются в

том, что сотрудники не знают о существующих политиках BYOD или забывают, что политики BYOD были им представлены.

Угроза ИБ: Неэффективные механизмы контроля безопасности. Механизмы безопасности мобильных устройств включают шифрование, аутентификацию, возможности удаленного уничтожения данных, программное обеспечение (ПО) для предотвращения вторжений и антивирусное ПО. Растущий уровень функциональности и производительность мобильных устройств вызвали всплеск проблем с безопасностью. Существующие механизмы безопасности не всегда адаптированы к новым мобильным и облачным технологиям. На большинстве мобильных устройств отсутствуют расширенные функции безопасности, а сотрудники даже отключают существующие базовые функции, такие как управление паролем. ИТ-отделы часто не владеют информацией об установленном или обновленном антивирусном программном обеспечении на мобильном устройстве сотрудников [16].

Угроза ИБ: Отсутствие осведомленности о мерах ИБ. Осведомленность о безопасности определяется как отношение и знания сотрудников о защите информационных активов своей организации и о том, что они должны соответствующим образом реагировать при возникновении угроз.

В организациях, где отсутствует осведомленность о мерах ИБ, сотрудники не обращают внимания на очевидные риски безопасности, такие, как вирусы или кража интеллектуальной собственности в их повседневной трудовой деятельности. Несмотря на принятые превентивные меры, такие, как защита от вредоносных программ и брандмауэр, эти меры могут помочь лишь в решении части проблем, поскольку наивные и неосведомленные сотрудники могут подвергнуть организацию дорогостоящим ошибкам [17]. Таким образом, последствия отсутствия осведомленности о мерах ИБ

представляют собой угрозу, поэтому обучение методам ИБ стало важнейшим инструментом для противодействия киберугрозам.

Угроза ИБ: Небезопасные сети. Сотрудники все чаще получают доступ к внутренним сетям, таким, как корпоративные интрасети и серверы электронной почты, через свои собственные устройства, когда они находятся вне рабочей среды.

Поскольку эти сети часто не защищены, это может открыть устройство и косвенно организацию для атак. Атаки могут происходить в форме спуфинга сети, акта маскировки сообщения из неизвестного источника под сообщение из известного, надежного источника для получения доступа к конфиденциальным данным или запуска атак типа «отказ в обслуживании» [18].

Например, в феврале 2018 году злоумышленниками была осуществлена DDoS-атака на GitHub, с использованием IP-спуфинга. Интернациональная группа хакеров подделала IP-адрес GitHub и реализовала интенсивную атаку. В результате этой атаки сервис был недоступен в течение одной трети часа. Для возобновления функционирования сервиса GitHub было произведено перенаправление трафика на центры очистки [19].

Методика научного исследования

Качественный метод исследования основывался на интерпретации результатов интервьюирования сотрудников различных организаций. В целевую группу были включены ИТ-директора, руководители ИТ-отделов и сотрудники, работающие в ИТ-отделе. ИТ-директор принимает решения и определяет политику ИБ, поэтому обладает соответствующей информацией, необходимой для решения вопросов, связанных с политикой использования BYOD-устройств, в то время как другие участники выборки участвуют в повседневных операциях в области ИТ, включая устранение проблем безопасности информационных систем. В целевую группу для исследования

было включено шестнадцать специалистов. Эти люди ежедневно работали и сталкивались с проблемами безопасности информационных систем, поэтому они были лучше информированы о масштабах проблем, с которыми сталкивается компания, предоставляющая финансовые услуги. Знания и опыт участников в области обслуживания ИТ-систем были основными критериями для включения в исследование. После составления графика опрос проводился с помощью программного обеспечения для защищенных видеоконференций и записывался на компьютер.

Затем интервью были расшифрованы с использованием автоматизированной системы распознавания речи. Собранные данные прошли шесть этапов тематического анализа: ознакомление, кодирование, создание тем, обзор тем, определение и наименование тем и написание отчета.

Результаты научного исследования

В исследовании изучалось понимание сотрудниками компаний концепции BYOD. Было выявлено, что все участники опроса хорошо понимают данную концепцию и BYOD-устройства используется в 87,5% организаций.

Сорок пять процентов организаций не участвуют в выборе BYOD-устройства, поэтому сотрудник может принести любой ноутбук, любое мобильное устройство. Использование различных устройств и операционных систем приводит к усложнению реализации мер ИБ.

Семьдесят процентов организаций ограничивают количество мобильных устройств, подключаемых к корпоративным информационным системам, так как это приводит к увеличению количества лицензий на программное обеспечение и усложнению контроля подключений.

Участники опроса дали различные ответы относительно существования или отсутствия политики BYOD. Десять участников сказали, что политика

ИБ BYOD реализована в их организации, два участника затруднились дать ответ и четыре участника ответили, что политика ИБ BYOD не документирована в их компании.

В ходе исследования оценивался уровень осведомленности сотрудников в области ИБ и периодичность проведения тренингов по освоению элементов политики ИБ. Выяснилось, что восемьдесят процентов организаций ежеквартально проводят тренинги и семинары по обеспечению ИБ для сотрудников. Однако, только в половине организаций проводится обучение ИБ при работе с BYOD-устройствами. В большей части компаний ежегодно проводятся обязательные тесты по ИБ, чтобы убедиться, что сотрудники владеют навыками соблюдения мер ИБ. Также в большинстве компаний часто тестируют реакцию сотрудников на потенциальные фишинговые атаки. Все участники согласились с тем, что различные виды тестирования сотрудников внесли значительный вклад в обеспечение ИБ.

Была исследована реакция сотрудников на внедрение корпоративных продуктов для обеспечения ИБ на их личных устройствах. Участники опроса заявили, что у некоторых сотрудников компании сложилось негативное отношение к мерам ИБ BYOD. Сотрудники не всегда готовы устанавливать специализированное программное обеспечение (ПО) для обеспечения необходимого уровня ИБ BYOD. Это было связано с тем, что существует мнение о том, что через данное ПО организация может иметь доступ к личной информации сотрудников.

Произведен анализ влияние BYOD на сетевую безопасность. Большинство участники подтвердили, что они уверены в том, что вычислительная сеть компании сохранила достаточный уровень ИБ после внедрения концепции BYOD. Необходимый уровень ИБ был в основном достигнут путем использования подключения к сети через VPN, с многофакторной аутентификацией и применением протокола IKEv2.

Было выявлено, что девяносто процентов организаций используют системы предотвращения вторжений и обнаружения для защиты сетевой инфраструктуры, а также демилитаризованные зоны для защиты периметра организации и дополнительного уровня безопасности локальной вычислительной сети компании.

Было произведено консолидирование информации по мерам ИБ BYOD и меры по уменьшению последствий кражи или потери BYOD-устройства.

По результатам опроса выявлено, что внедрение систем управления мобильным устройствами (СУМ) было ключевым решением, используемым для защиты устройств сотрудников и управления ими. Примером отечественного СУМ является «СУМ Оптимум защита», выпускаемая ООО «ИРЦЭ» [20]. СУМ позволяет хранить корпоративную информацию, хранящуюся на устройствах, в специальном контейнере, и в случае сообщения о потере или краже устройства контейнер безвозвратно стирается с устройства, чтобы защититься от потенциальной потери данных. Для получения доступа к корпоративным ресурсам компании, сотрудникам необходимо сначала установить ПО СУМ на свое мобильное устройство.

Было выявлено, что многие компании широко используют облачные решения. Для управления и защиты данных, хранящихся в облаке, в 65% этих компаний были внедрены брокеры безопасного доступа в облако - CASB. CASB (Cloud Access Security Broker) – это универсальный компонент ИБ, который позволяет специалистам службы ИБ выявлять потенциальные риски и поддерживать высокий уровень защиты.

CASB помогает обеспечить безопасность работы с облачными приложениями на устройствах сотрудников.

Выводы

В данном исследовании проанализированы основные уязвимости ИБ, связанные с использованием концепции BYOD: скомпрометированные

данные, атаки вредоносных программ, злонамеренные инсайдеры, теневые ИТ ресурсы, отсутствие политик BYOD, неэффективные механизмы контроля безопасности, оотсутствие осведомленности о мерах ИБ, небезопасные сети.

Необходимо использовать системы СУМ (MDM), которые позволяют отслеживать потерянные или украденные устройства, удаленно стирать корпоративную информацию на них для предотвращения несанкционированного доступа (НСД) к конфиденциальным данным. Также для защиты мобильных устройств сотрудники должны использовать уникальные пароли для защиты от НСД. Также на BYOD-устройства следует устанавливать антивирус или защиту от вредоносных программ. Для успешного внедрения решений по защите ИБ, организациям требуется меры по повышению лояльности сотрудников к своей компании.

Концепция BYOD может быть полезной, но может представлять серьезную угрозу для организации, поскольку ИТ-отдел или организация не всегда имеют возможности отслеживать количество и тип устройств, входящих в корпоративную сеть. Повышение уровня осведомленности персонала о мерах ИБ при работе с мобильными устройствами не всегда гарантирует удовлетворительные результаты. Поскольку области, подверженные рискам ИБ, постоянно расширяются, непрерывное обучение сотрудников методам поддержания ИБ становится жизненно важным для того, чтобы сотрудники не удовлетворялись существующими знаниями и практиками в области безопасности, а культивировали культуру осведомленности о безопасности внутри организации.

Большую роль в обеспечении ИБ играет политика BYOD, которая устанавливает жесткие ограничения, связанные с использованием активов компании, и описывает все действия, которые разрешены на устройствах, когда они используются в корпоративных информационных системах.

Ограничения на устройствах могут включать контроль паролей, включение определенных параметров безопасности, установку определенного программного обеспечения и антивируса, управление интерфейсами беспроводной сети.

Было выявлено, что самой большой угрозой безопасности, связанной с использованием концепции BYOD, является потеря конфиденциальных данных компании. Последствия этих угроз могут оказать серьезное влияние на репутацию организации, могут привести к потенциальному закрытию бизнеса и утечке конфиденциальных данных клиентов организации. Также не во всех организациях существует политика ИБ BYOD.

Выяснилось, что для обеспечения безопасности периметра информационной инфраструктуры прилагаются большие усилия. Однако, необходимо учитывать, что по мере развития технологий возникают все новые и новые угрозы. Поэтому не реже чем каждые шесть месяцев необходимо проводить аудит систем ИБ и пересмотр политики ИБ, и, в том числе, политики использования BYOD-устройств.

Литература

1. Семеко Г.В. Информационная безопасность в финансовом секторе: Киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1. С. 77-96.
2. Palanisamy R., Norman A. A., Mat Kiah M. L. BYOD policy compliance: Risks and strategies in organizations // Journal of Computer Information Systems. 2022. № 62(1). P. 61-72.
3. Ибрагимова З.М., Батчаева З.Б., Ткаченко А.Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010/.

4. Филяк П.Ю., Изъюров А.А. Информационная безопасность при использовании мобильных устройств в корпоративной среде // Информация и безопасность. 2016. Т. 19. № 4. С. 579-582.

5. Downer K., Bhattacharya M. BYOD security: A study of human dimensions // Informatics, 2022, №9 URL: doi.org/10.3390/informatics9010016/.

6. Chen H., Li Y., Chen L., Yin, J. Understanding employees' adoption of the bring-your-own-device (BYOD): The roles of information security-related conflict and fatigue // Journal of Enterprise Information Management. 2021. № 34. P. 770-792.

7. Miura H., Abukawa S., Kimura T., Hirata K. Modeling of malware diffusion with mobile devices in intermittently connected networks // Asia-Pacific Signal and Information Processing Association Annual Summit and Conference. 2022. P. 1756-1759.

8. Большое банковское ограбление: APT-кампания Carbanak. URL: securelist.ru/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/25106/

9. Zhang R., Bello A., Foster, J. L. BYOD security: Using dual process theory to adapt effective security habits in BYOD // Proceedings of the Future Technologies Conference. 2022. V. 2. P. 372-386.

10. Вайт С. Не боритесь с теневыми ИТ, а сделайте их своими "соратниками" // Директор информационной службы. 2016. № 8. С. 36.

11. Эдвардс Д. 7 способов оказаться в выигрыше, используя теневые ИТ // Директор информационной службы. 2018. № 3. С. 47.

12. Кулишова А. В. Анализ рисков использования в компаниях теневых облачных приложений // Экономика. Право. Инновации. 2017. № 1. С. 80-85.

13. Останина Е. А. Информационная безопасность при реализации концепции BYOD // Человеческий капитал. 2019. № 12. С. 131-141.

14. Смаглюк Е. В., Бондарь К. М. Исследование угроз безопасности корпоративных информационных систем, компонентами которых являются

мобильные устройства // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2022. Т. 1. С. 276-282.

15. BYOD бьет по безопасности. URL: comnews.ru/content/207577/2020-06-11/2020-w24/byod-bet-bezopasnosti

16. Мобильные угрозы и методы борьбы с ними. URL: securitylab.ru/analytics/501302.php/.

17. Mwim E. N., Mtsweni J. Systematic review of factors that influence the cybersecurity culture // Human Aspects of Information Security and Assurance. 2022. P. 147–172

18. Шепелев А.Н. , Букатов А.А. , Пыхалов А.В. , Березовский А.Н. Анализ подходов и средств обработки сервисных журналов // Инженерный вестник Дона, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n4y2013/1966/.

19. Что такое IP-спуфинг и как с ним бороться. URL: kaspersky.ru/resource-center/threats/ip-spoofing/.

20. Система Управления Мобильными Устройствами «ОПТИМУМ Защита». URL: dedicorp.ru/optimum-defence/.

References

1. Semeko G.V. Social'nye novacii i social'nye nauki. 2020. № 1. pp. 77-96.

2. Palanisamy R., Norman A. A., Mat Kiah M. L. Journal of Computer Information Systems. 2022. № 62(1). pp. 61-72.

3. Ibragimova Z.M., Batcha Eva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010/.

4. Filjak P.Ju., Iz'jurov A.A. Informacija i bezopasnost'. 2016. T. 19. № 4. pp. 579-582.

5. Downer K., Bhattacharya M. Informatics, 2022, №9. URL: doi.org/10.3390/informatics9010016/.

6. Chen H., Li Y., Chen L., Yin, J. Journal of Enterprise Information Management. 2021. № 34. pp. 770-792.

7. Miura H., Abukawa S., Kimura T., Hirata K. Asia-Pacific Signal and Information Processing Association Annual Summit and Conference. 2022. pp. 1756-1759.

8. Bol'shoe bankovskoe ograblenie: APT-kampanija Carbanak. [The Great Bank Robbery: the Carbanak APT]. URL: securelist.ru/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/25106/.

9. Zhang R., Bello A., Foster, J. L. Proceedings of the Future Technologies Conference. 2022. V. 2. pp. 372-386.

10. Vajt S. Direktor informacionnoj sluzhby. 2016. № 8. P. 36.

11. Jedvards D. Direktor informacionnoj sluzhby. 2018. № 3. P. 47.

12. Kulishova A. V. Jekonomika. Pravo. Innovacii. 2017. № 1. pp. 80-85.

13. Ostanina E. A. Chelovecheskij kapital. 2019. № 12. pp. 131-141.

14. Smagljuk E. V., Bondar' K. M. Nauchno-tehnicheskoe i jekonomicheskoe sotrudnichestvo stran ATR v XXI veke. 2022. T. 1. pp. 276-282.

15. BYOD b'et po bezopasnosti. [BYOD hits security]. URL: comnews.ru/content/207577/2020-06-11/2020-w24/byod-bet-bezopasnosti/.

16. Mobil'nye ugrozy i metody bor'by s nimi. [Mobile threats and methods of dealing with them]. URL: securitylab.ru/analytics/501302.php/.

17. Mwim E. N., Mtsweni J. Human Aspects of Information Security and Assurance. 2022. pp. 147–172.

18. Shepelev A.N., Bukatov A.A., Pyhalov A.V., Berezovskij A.N. Inzhenernyj vestnik Dona, 2022, №11. URL: ivdon.ru/ru/magazine/archive/n4y2013/1966/.

19. Chto takoe IP-spufing i kak s nim borot'sja. [What is IP spoofing and how to deal with it]. URL: kaspersky.ru/resource-center/threats/ip-spoofing

20. Sistema Upravlenija Mobil'nymi Ustrojstvami «OPTIMUM Zashhita». [Mobile Device Management System OPTIMUM Protection]. URL: dedicorp.ru/optimum-defence/.