УДК *004.056*

И.С. Рябов, Л.В. Аршинский

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЙ МАЛОГО БИЗНЕСА

Аннотация. *В данной статье рассматриваются основные проблемы обеспечения информационной безопасности в малом бизнесе, анализируются существующие методы защиты, с акцентом на их применимость и эффективность в условиях ограниченных ресурсов, а также предлагаются конкретные, практико-ориентированные рекомендации, направленные на минимизацию возможных рисков и повышение общего уровня защищенности. Предложены практические подходы, включающие разработку минимальных отраслевых сценариев защиты информации и введение модели гибридных ролей сотрудников с элементами ответственности за обеспечение безопасности, что позволяет минимизировать затраты и повысить устойчивость предприятий к угрозам.*

Ключевые слова: *информационная безопасность, малый бизнес, защита данных, риск информационной безопасности*

I.S. Ryabov, L.V. Arshinskiy

Irkutsk State Transport University, Irkutsk, the Russian Federation

THE PROBLEM OF ENSURING INFORMATION SECURITY FOR SMALL BUSINESSES

Abstract. *This article examines the main problems of ensuring information security in small businesses, analyzes existing protection methods, with an emphasis on their applicability and effectiveness in conditions of limited resources, and offers specific, practice-oriented recommendations aimed at minimizing possible risks and increasing the overall level of security. Practical approaches are proposed, including the development of minimal industry scenarios for information protection and the introduction of a model of hybrid employee roles with elements of responsibility for security, which minimizes costs and increases the resilience of enterprises to threats.*

Keywords: *information security, small business, data protection, information security risk*

Введение

Информационная безопасность является важной составляющей успешного функционирования любого предприятия, вне зависимости от его масштаба. Однако малые предприятия сталкиваются с особыми трудностями при обеспечении защиты данных, что делает их уязвимыми перед современным спектром угроз, эволюционирующих с высокой скоростью.

Современный бизнес становится все более зависимым от информационных технологий [1]. Данные являются важнейшим активом, от сохранности которого зависит эффективность работы компании. Внедрение цифровых решений предоставляет малому бизнесу возможности для развития, однако также несет в себе значительные угрозы, связанные с кибератаками, утечками данных и мошенническими действиями. В отличие от крупных корпораций, малые предприятия зачастую не только не имеют специализированных отделов информационной безопасности и не могут выделить значительные бюджеты на защиту данных, но и вовсе лишены даже минимального штата специалистов в этой области. В большинстве случаев в компании нет не только сотрудника, отвечающего за информационную безопасность, но даже системного администратора, что делает их особенно уязвимыми для злоумышленников.

Проблема информационной безопасности для малого бизнеса становится особенно актуальной в условиях роста числа информационных атак. В последние годы наблюдается значительное увеличение атак на малые и средние предприятия, так как злоумышленники осознают их слабую защищенность. Согласно данным «Лаборатории Касперского», с января

по апрель 2024 года общее количество заражений в секторе малого и среднего бизнеса составило 138 046 случаев, что на 5% больше по сравнению с аналогичным периодом 2023 года. Этот рост свидетельствует о повышенном интересе киберпреступников к малым предприятиям, которые часто имеют менее защищенные ИТ-инфраструктуры [2]. Многие предприятия считают себя слишком маленькими, чтобы быть интересными для хакеров, но это опасное заблуждение [3]. Важно понимать, что обеспечение информационной безопасности – это не разовая мера, а постоянный процесс, требующий регулярного мониторинга, обновления и обучения персонала.

Цель данной работы заключается в выполнении обзора подходов к защите информации на предприятиях малого бизнеса и формировании рекомендаций по обеспечению защиты информации с учетом их основных особенностей. В частности, предлагается адаптировать меры обеспечения информационной безопасности для малого бизнеса на основе известных подходов, применяемых в крупных предприятиях. К особенностям малого предприятия относятся: ограниченность бюджета, недостаток квалифицированных кадров в области информационной безопасности, отсутствие массовых целенаправленных атак (что снижает приоритет вопросов информационной безопасности в глазах владельцев бизнеса), высокая зависимость от внешних IT-провайдеров и облачных сервисов, ограниченные возможности для проведения регулярных аудитов и оценки рисков, а также низкий уровень формализации бизнес-процессов и процедур безопасности [4]. Все эти факторы требуют разработки специфических подходов к построению системы защиты, ориентированной на минимизацию рисков при максимально эффективном использовании ограниченных ресурсов.

Основные угрозы информационной безопасности

Одной из самых серьезных и часто недооцениваемых проблем, с которыми сталкиваются малые предприятия, является недостаточная осведомленность сотрудников в вопросах информационной безопасности. Часто именно человеческий фактор становится причиной успешного взлома системы или утечки данных. Работники могут использовать слабые пароли [5], не проверять подлинность писем и документов, а также становиться жертвами социальной инженерии, когда злоумышленники обманным путем получают доступ к конфиденциальной информации. Например, злоумышленник может представиться сотрудником технической поддержки и попросить предоставить пароль для "устранения неисправности" или отправить электронное письмо, замаскированное под уведомление от банка, с просьбой перейти по ссылке и ввести свои учетные данные [6].

Еще одной распространенной и опасной угрозой является вредоносное программное обеспечение (ВПО). Современные вирусы, трояны, черви и программы-вымогатели могут проникать в систему предприятия различными путями, например, через зараженные веб-сайты, электронную почту или USB-накопители [7]. Попав в систему, ВПО может блокировать доступ к файлам, шифровать данные (требуя выкуп за их восстановление) или похищать конфиденциальную информацию для дальнейшего использования в преступных целях [8]. В результате атаки вредоносного ПО компания может потерять важные данные, нарушить свою деятельность, понести значительные финансовые убытки, а также нанести ущерб своей репутации. Восстановление системы после заражения ВПО может потребовать значительных финансовых затрат, времени и усилий. Так, атака программы-вымогателя (шифровальщика) может парализовать работу компании на несколько дней или даже недель, что приведет к потере клиентов и прибыли.

Использование устаревшего программного обеспечения также представляет серьезную опасность для бизнеса. Многие компании продолжают работать на старых версиях операционных систем и программ, которые больше не поддерживаются разработчиками. Это создает уязвимости, которыми могут воспользоваться хакеры для проникновения в систему и получения доступа к данным. Регулярное и своевременное обновление программного обеспечения – одно из ключевых требований для обеспечения надежной защиты.

Одним из слабых мест в системе безопасности малых предприятий является недостаточная защита облачных сервисов. Все больше компаний, стремясь к повышению эффективности и снижению затрат, используют облачные хранилища и приложения для хранения данных, обмена информацией и совместной работы. Однако многие из них не уделяют должного внимания обеспечению безопасности этих облачных сервисов. Использование слабых паролей, отсутствие многофакторной аутентификации и пренебрежение базовыми мерами безопасности значительно упрощают злоумышленникам доступ к корпоративным данным. Малые предприятия зачастую не внедряют надежные механизмы защиты учетных записей, позволяя сотрудникам использовать предсказуемые или повторяющиеся пароли. Кроме того, отсутствие контроля над доступом к облачным сервисам может привести к утечке конфиденциальной информации или компрометации учетных записей.

Методы защиты и рекомендации

Для эффективного обеспечения информационной безопасности малые предприятия должны разработать и внедрить четкую и всеобъемлющую стратегию защиты данных, учитывающую специфику их деятельности и доступные ресурсы.

В первую очередь необходимо внедрить политику информационной безопасности – основополагающий документ, который регламентирует процессы обеспечения информационной безопасности в организации. Политика должна включать в себя основные принципы, цели и стандарты безопасности [9], а также конкретные требования и рекомендации для защиты информационных активов компании от рисков, возникающих в результате реализации угроз информационной безопасности. Политика должна охватывать все аспекты информационной безопасности, включая физическую безопасность, защиту сети, защиту данных, управление доступом, реагирование на инциденты и обучение сотрудников.

Обучение сотрудников является важным элементом обеспечения безопасности. Регулярное проведение тренингов по вопросам информационной безопасности поможет повысить осведомленность персонала и снизить вероятность реализации атак. Работники должны понимать, как распознавать подозрительные письма, почему нельзя использовать простые пароли и какие меры необходимо предпринимать для защиты конфиденциальной информации [10].

Для защиты данных следует использовать современные и надежные программные и аппаратные средства защиты информации, включая:

1) Антивирусные программы. Для обнаружения и блокирования вредоносного программного обеспечения (вирусов, троянов, червей и т.д.). Важно выбирать антивирусные решения от известных и надежных поставщиков (например, Kaspersky) и регулярно обновлять антивирусные базы. Рассмотрите возможность использования централизованной системы управления антивирусной защитой для упрощения администрирования и мониторинга.

2) Межсетевые экраны. Для контроля сетевого трафика и предотвращения несанкционированного доступа к внутренним ресурсам компании. Можно использовать как аппаратные, так и программные межсетевые экраны. Важно правильно настроить межсетевой экран, чтобы разрешать только необходимый трафик и блокировать весь остальной.

3) Системы обнаружения и предотвращения вторжений. Для выявления и блокирования подозрительной активности в сети. IDS обнаруживает подозрительную активность, а IPS автоматически блокирует ее. Эти системы могут помочь обнаружить и предотвратить атаки, которые не были обнаружены межсетевым экраном или антивирусной программой.

4) Системы защиты от утечек данных. Для предотвращения несанкционированной передачи конфиденциальной информации за пределы компании. DLP-системы могут

отслеживать и блокировать передачу данных через электронную почту, веб-браузеры, USB-накопители и другие каналы.

5) Многофакторная аутентификация. Для усиления защиты учетных записей пользователей и предотвращения несанкционированного доступа к системам и данным.

Важно не только установить такие программы и устройства, но и регулярно их обновлять, правильно настраивать и контролировать их работу, чтобы они могли эффективно справляться с новыми и постоянно появляющимися угрозами.

Ограничение прав доступа сотрудников к данным также играет важную роль в обеспечении безопасности. Важно предоставлять каждому сотруднику доступ только к той информации, которая ему действительно необходима и достаточна для выполнения его должностных обязанностей (принцип наименьших привилегий). Это позволит снизить риск утечки данных и минимизировать возможный ущерб при атаке.

Резервное копирование данных является одной из наиболее эффективных мер по защите информации от потери или повреждения. Малые предприятия должны регулярно создавать резервные копии критически важных данных (например, баз данных, финансовых документов, клиентской информации) и хранить их в безопасном месте, отделенном от основной системы. Рассмотрите возможность использования облачных сервисов резервного копирования для дополнительной защиты данных. В случае утраты информации из-за атак, аппаратного сбоя, человеческой ошибки или стихийного бедствия, восстановление данных из резервной копии позволит избежать значительных потерь и быстро восстановить работоспособность компании. Регулярно проверяйте работоспособность системы восстановления данных из резервных копий, чтобы убедиться, что она работает правильно.

Для повышения эффективности обеспечения информационной безопасности в условиях ограниченных ресурсов малого бизнеса предлагается внедрение следующих оригинальных подходов:

1.Минимальные сценарии защиты для разных типов малого бизнеса

Учитывая специфику деятельности предприятий, целесообразно разработать типовые минимальные сценарии защиты информации, ориентированные на особенности каждой отрасли.

Например:

– кафе и рестораны: особое внимание должно быть уделено защите POS-терминалов (систем приёма платежей), сегментации корпоративной и гостевой сетей Wi-Fi, а также регулярному обновлению программного обеспечения кассовых аппаратов.

– юридические фирмы и бухгалтерские компании: приоритетом является шифрование клиентских данных, организация строгого контроля доступа к документам и регулярное резервное копирование критической информации.

– магазины розничной торговли: основное внимание необходимо уделить защите кассовых систем, ограничению физического доступа к рабочим станциям и внедрению базовой антивирусной защиты всех устройств.

– сервисные и консультационные компании: ключевыми мерами являются обеспечение безопасности электронной почты, обучение сотрудников правилам работы с конфиденциальной информацией и использование многофакторной аутентификации для доступа к облачным сервисам.

Подобная адаптация мер безопасности позволяет малым предприятиям учитывать отраслевые риски, рационально использовать ограниченные ресурсы и существенно повысить общий уровень защищенности.

2. Гибридные роли сотрудников с функциями обеспечения информационной безопасности

В условиях ограниченных ресурсов многие малые предприятия не могут позволить себе нанять отдельного специалиста по информационной безопасности. В этой связи предлагается модель гибридных ролей, при которой один из существующих сотрудников

компании совмещает выполнение базовых задач по информационной безопасности с основной деятельностью.

Рекомендуется официально назначить сотрудника ответственного за информационную безопасность из числа IT-администраторов, офис-менеджеров или технических специалистов. Для облегчения выполнения этой функции необходимо разработать четкий регламент и пошаговый чек-лист, включающий следующие задачи:

– контроль регулярного обновления программного обеспечения и антивирусных баз;

– обеспечение соблюдение регламентов и политики информационной безопасности;

– регулярное создание и проверку резервных копий;

– проведение инструктажей сотрудников по основам информационной безопасности;

– фиксацию и первичный анализ инцидентов безопасности с последующим докладом руководству.

Такой подход позволяет организовать начальный уровень информационной безопасности даже в условиях минимальных затрат, без необходимости кардинального изменения организационной структуры предприятия. При этом наличие регламентированной ответственности значительно снижает вероятность реализации угроз, связанных с человеческим фактором

Выбор средств защиты информации исходя из бюджета

В малом бизнесе затраты на IT и информационную безопасность (ИБ) чаще всего идут из одного бюджета, без выделения ИБ в отдельную статью расходов. Обычно компании закладывают на IT-инфраструктуру от 2% до 10% от выручки, а из этих средств на ИБ уходит 10–30%. Это позволяет определить ориентиры для планирования защиты в зависимости от размера бюджета:

1) Минимальный уровень IT-бюджета (2% от выручки = 100 000 руб.):

Затраты на ИБ: 10 000 – 15 000 руб.

– Антивирусные решения. (Dr. Web Security Space, Kaspersky Small Office Security) [11].

– Минимальная защита сети (например, роутер с базовыми настройками безопасности, ViPNet Client) [12].

– Резервное копирование данных. (Яндекс. Диск для бизнеса).

2) Средний IT-бюджет (5% = 250 000 руб.)

Затраты на ИБ: 40 000 – 75 000 руб.

– Лицензированные средства защиты (Kaspersky Endpoint Security, ViPNet Coordinator).

– Контроль доступа к данным (КриптоПро CSP, Рутокен).

– Обучение сотрудников основам информационной безопасности.

– Регулярное обновление ПО.

3) Максимальный IT-бюджет (10% от выручки = 500 000 руб.):

Затраты на ИБ: 100 000 – 150 000 руб.

– Мониторинг событий безопасности, аудит безопасности (MaxPatrol SIEM, Solar Dozor).

– Полноценная защита корпоративной сети (Континент 4.5 для построения защищённых сетей передачи данных).

– Регулярные пентесты (услуги от Positive Technologies).

– Нанятый или аутсорсинговый специалист по ИБ.

Выбор конкретных средств защиты должен базироваться на реальной оценке рисков и ценности обрабатываемой информации [13]. Рекомендуется проводить базовую категоризацию данных для определения приоритетов защиты, направляя ресурсы на наиболее критичные активы.

Дополнительные рекомендации для малого бизнеса.

- Проведение регулярных аудитов безопасности. Оценка уязвимостей и рисков поможет выявить слабые места в системе безопасности и принять меры по их устранению.

Можно привлекать сторонних специалистов для проведения аудита или использовать автоматизированные инструменты сканирования уязвимостей [14].

- Разработка плана реагирования на инциденты. План должен содержать четкие инструкции о том, что делать в случае кибератаки или утечки данных. Важно регулярно тестировать план, чтобы убедиться, что он работает эффективно.
- Использование надежных паролей и менеджеров паролей. Сотрудники должны использовать сложные и уникальные пароли для каждой учетной записи. Менеджеры паролей могут помочь генерировать и хранить надежные пароли.
- Шифрование данных. Шифрование данных защитит их от несанкционированного доступа, даже если они будут украдены. Шифруйте данные, хранящиеся на компьютерах, серверах и в облачных сервисах.

При разработке и внедрении мер по обеспечению информационной безопасности, малым предприятиям важно руководствоваться принципом необходимой достаточности. Это означает, что уровень защиты должен быть адекватен существующим рискам и возможностям компании. Не всегда требуется внедрять самые дорогие и сложные решения. В некоторых случаях можно успешно использовать бесплатные или недорогие инструменты и методы, особенно на начальном этапе. Например, бесплатные антивирусные программы могут обеспечить базовую защиту от вредоносного ПО, а открытые системы обнаружения вторжений могут помочь выявлять подозрительную активность в сети [15]. Важно тщательно оценить риски, определить наиболее критичные активы и сосредоточиться на их защите, используя доступные ресурсы максимально эффективно. Однако следует помнить, что бесплатные решения могут иметь ограничения по функциональности и поддержке, поэтому необходимо регулярно оценивать их эффективность и, при необходимости, переходить на более продвинутые решения. Главное – это не стоимость решения, а его соответствие потребностям компании и эффективность в защите данных. Важно также регулярно проводить оценку эффективности внедренных мер защиты и адаптировать их в соответствии с изменяющимися угрозами и возможностями компании.

Заключение

Информационная безопасность является важнейшим аспектом успешной и устойчивой работы малого бизнеса в современном цифровом мире. В условиях быстрого роста числа и сложности информационных угроз предприятия должны осознанно и ответственно подходить к защите своих данных, внедрять современные технологии и обучать персонал. Несмотря на ограниченные ресурсы, малый бизнес может эффективно защищать себя с помощью доступных и эффективных методов, таких как резервное копирование, своевременное обновление программного обеспечения, контроль доступа, многофакторная аутентификация и антивирусные решения. В рамках данной работы также предложены оригинальные практические рекомендации: разработка минимальных отраслевых сценариев защиты информации для разных типов малого бизнеса и реализация модели гибридных ролей сотрудников с элементами ответственности за информационную безопасность. Данные подходы позволяют повысить уровень защищенности организаций без существенного увеличения расходов и адаптировать систему защиты к специфике их деятельности.

Обеспечение информационной безопасности – это не разовое мероприятие, а непрерывный и динамичный процесс, который требует регулярного мониторинга, постоянной адаптации к новым вызовам и угрозам, а также активного участия всего персонала компании. Игнорирование вопросов информационной безопасности может привести к катастрофическим последствиям для малого бизнеса, включая потерю клиентов, финансовые убытки и даже банкротство. Только комплексный и системный подход к обеспечению информационной безопасности позволит малым предприятиям минимизировать риски, защитить свои данные, сохранить репутацию и обеспечить устойчивое развитие в условиях цифровой экономики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ефремов Н.А., Мужжавлева Т.В. Процессы информатизации экономики и информационная безопасность // Экономика и предпринимательство. 2023. № 3. С. 287-294.
2. Кибербезопасность малого и среднего бизнеса: анализ тенденции [Электронный ресурс]. – URL: https://securelist.ru/smb-threat-report-2024/109844/ (дата обращения: 15.02.2025).
3. ИБ малого и среднего бизнеса – статистика против заблуждений [Электронный ресурс]. – URL: https://www.evraas.ru/resources/ib-malogo-i-srednego-biznesa-statistika-protiv-zabluzhdeniy/ (дата обращения: 15.02.2025).
4. Пузанова Г.А., Пузанов А.А. [Электронный ресурс] Особенности обеспечения информационной безопасности предприятий малого и среднего бизнеса // Актуальные проблемы авиации и космонавтики. 2013. №9. –URL: https://cyberleninka.ru/article/n/osobennosti-obespecheniya-informatsionnoy-bezopasnosti-predpriyatiy-malogo-i-srednego-biznesa (дата обращения: 15.02.2025).
5. Иванов М.Ю., Сыготина М.В., Вахрушева М.Ю., Надршин В. В. Информационная безопасность современного предприятия = Information Security of Advanced Company: Password Protection: парольная защита // Защита информации. Инсайд. 2022. № 6. С. 62-66.
6. Список основных ИТ-угроз от ваших подчиненных – как контролировать работу сотрудников [Электронный ресурс]. –URL: https://www.zeluslugi.ru/info-czentr/stati/kak-izbezhat-vnutrennih-it-ugroz (дата обращения: 15.02.2025).
7. Догучаева С.М. Анализ современных проблем информационной безопасности в российских компаниях // Риск: ресурсы, информация, снабжение, конкуренция. 2022. № 2. С. 65-68.
8. Защита малого бизнеса от киберугроз [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-security (дата обращения: 15.02.2025).
9. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации от 27 июля 2006 г. № 149-ФЗ». / СПС «КонсультантПлюс». [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 15.02.2025).
10. Незнание принципов ИБ не освобождает от ответственности [Электронный ресурс]. – URL: https://habr.com/ru/companies/trendmicro/articles/438250/ (дата обращения: 15.02.2025).
11. IT-БЕЗОПАСНОСТЬ МАЛОГО БИЗНЕСА: ПРАКТИЧЕСКОЕ РУКОВОДСТВО [Электронный ресурс]. – URL: https://media.kaspersky.com/ru/business-security/kaspersky-small-business-it-security-practical-guide-ru.pdf (дата обращения: 15.02.2025).
12. Информационная безопасность в малом и среднем бизнесе. Алгоритмы и действия [Электронный ресурс]. – URL: https://moluch.ru/archive/315/71976/ (дата обращения: 15.02.2025).
13. Глухов Н.И. Оценка информационных рисков предприятия: учебное пособие. Иркутск: ИРГУПС, 2013. 148 с.
14. Информационная безопасность предприятий [Электронный ресурс]. – URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij/ (дата обращения: 15.02.2025).
15. Нам нечего терять! Безопасность для самых маленьких… компаний [Электронный ресурс]. – URL: https://habr.com/ru/companies/regionsoft/articles/555036/ (дата обращения: 15.02.2025).

REFERENCES

1. Efremov N. A. Processes of informatization of economics and information security / N. A. Efremov, T. V. Muzhyavleva. *Economics and Entrepreneurship*, 2023, No. 3, pp. 287-294.

2. Cybersecurity of small and medium-sized businesses: trend analysis [Electronic resource]. – URL: https://securelist.ru/smb-threat-report-2024/109844 / (date of access: 02/15/2025).

3. Information security of small and medium–sized businesses - statistics against misconceptions [Electronic resource]. – URL: https://www.evraas.ru/resources/ib-malogo-i-srednego-biznesa-statistika-protiv-zabluzhdeniy / (date of access: 02/15/2025).

4. Puzanova G. A., Puzanov A. A. [Electronic resource] Features of ensuring information security of small and medium-sized businesses. *Actual problems of aviation and cosmonautics*. 2013. No.9. URL: https://cyberleninka.ru/article/n/osobennosti-obespecheniya-informatsionnoy-bezopasnosti-predpriyatiy-malogo-i-srednego-biznesa (date of request: 02/15/2025).

5. Ivanov M.Y., Sygotina M.V., Vakhrusheva M.Y., Nadrshin V.V. Information security of a modern enterprise = Information Security of an Advanced Company: Password Protection: password protection. *Information protection. Insid*, 2022, No. 6, pp. 62-66.

6. List of the main IT threats from your subordinates – how to control the work of employees [Electronic resource]. – URL: https://www.zeluslugi.ru/info-czentr/stati/kak-izbezhat-vnutrennih-it-ugroz (date of request: 02/15/2025).

7. Doguchaeva S. M. Analysis of modern information security problems in Russian companiesэ. *Risk: resources, information, supply, competition*, 2022, No. 2, pp. 65-68.

8. Protection of small business from cyber threats [Electronic resource] URL: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-security (date of request: 02/15/2025).

9. Federal Law of the Russian Federation No. 149-FZ of July 27, 2006 on Information, Information Technologies and Information Protection. / SPS "ConsultantPlus". [electronic resource]. – URL http://www.consultant.ru/document/cons_doc_LAW_61798 (date of access: 02/15/2025).

10. Ignorance of the principles of information security does not exempt from responsibility [Electronic resource]. – URL: https://habr.com/ru/companies/trendmicro/articles/438250 / (date of access: 02/15/2025).

11. IT SECURITY FOR SMALL BUSINESSES: PRACTICAL GUIDE [Electronic resource]. – URL: https://media .kaspersky.com/ru/business-security/kaspersky-small-business-it-security-practical-guide-ru.pdf (date of reference: 02/15/2025).

12. Information security in small and medium-sized businesses. Algorithms and actions [Electronic resource]. – URL: https://moluch.ru/archive/315/71976 (date of reference: 02/15/2025).

13. Glukhov N.I. Assessment of information risks of an enterprise: a textbook. Irkutsk: IRGUPS, 2013. 148 p.

14. Information security of enterprises [Electronic resource]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-predpriyatij / (date of request: 02/15/2025).

15. We have nothing to lose! Security for the smallest... companies [Electronic resource]. – URL: https://habr.com/ru/companies/regionsoft/articles/555036 (date of access: 02/15/2025).

Информация об авторах

Рябов Илья Сергеевич – магистрант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: ryabov21022002@gmail.com.

Аршинский Леонид Вадимович – д.т.н., доцент, профессор кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: arshinsky_lv@irgups.ru.

Information about the author

Ilya Sergeevich Ryabov – master's student of department “Information Systems and Information Security”, Irkutsk State Transport University, Irkutsk, e-mail: ryabov21022002@gmail.com.

Leonid Vadimovich Arshinskiy – Doctor of Technical Science, professor of department “Information Systems and Information Security”, Irkutsk State Transport University, Irkutsk, e-mail: arshinsky_lv@irgups.ru.