УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДНЕГО БИЗНЕСА ПРИ ИСПОЛЬЗОВАНИИ СОТРУДНИКАМИ СРЕДСТВ СВЯЗИ

Рахым М.Р.
магистрант, К.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана қ., Қазақстан Республикасы

Шайханова А.К.
PhD, К.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана қ., Қазақстан Республикасы

Алтынбек С.А.
PhD, К.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана қ., Қазақстан Республикасы

В данной статье рассматриваются основные угрозы безопасности для субъектов среднего бизнеса, возникающие в результате использования сотрудниками различных средств связи. Особое внимание уделяется вопросам кибербезопасности, рискам утечки данных, а также правовым аспектам защиты информации. Анализируются современные методы защиты корпоративных данных и разрабатываются рекомендации по минимизации угроз.

Ключевые слова: Кибербезопасность, утечка данных, средний бизнес, информационная безопасность, средства связи, законодательные требования, защита корпоративных данных, предотвращение атак, информационные технологии, удаленная работа.

Введение. Средний бизнес играет важную роль в экономике, однако он подвержен значительным угрозам безопасности, связанным с использованием средств связи сотрудниками. Современные технологии, включая мобильные устройства, мессенджеры и облачные сервисы, упрощают рабочие процессы, но при этом создают уязвимости для корпоративных данных. В данной статье проводится исследование ключевых проблем безопасности и предлагаются меры по их предотвращению.

Средний бизнес является важной частью экономики, обеспечивая рабочие места и способствуя развитию различных отраслей. Однако, с развитием цифровых технологий и активным использованием средств связи сотрудниками, компании сталкиваются с новыми вызовами в области безопасности. Современные технологии, такие как мобильные устройства, облачные сервисы и мессенджеры, существенно облегчают бизнес-процессы,

но в то же время создают уязвимости, связанные с утечкой данных, кибератаками и нарушением нормативных требований.

Одним из ключевых аспектов обеспечения безопасности в организациях среднего бизнеса является контроль за использованием корпоративных и личных средств связи. Неконтролируемое применение незащищенных каналов связи может привести к утечке конфиденциальной информации, что представляет угрозу для компании и её клиентов. Кроме того, нарушения в обработке персональных данных могут повлечь за собой серьезные штрафные санкции и подорвать доверие к организации.

В данной статье анализируются основные проблемы обеспечения безопасности субъектов среднего бизнеса в контексте использования сотрудниками средств связи. Рассматриваются современные методы защиты информации, анализируются потенциальные угрозы и предлагаются рекомендации по минимизации рисков, связанных с цифровой безопасностью.

1. Основные угрозы безопасности

1.1. Киберугрозы

Средний бизнес часто становится жертвой кибератак, таких как фишинг, вредоносное ПО и атаки типа "человек посередине" [1]. Недостаточная осведомленность сотрудников и слабая защита информационных систем увеличивают риски компрометации данных.

Киберугрозы представляют собой одну из наиболее серьезных проблем в сфере информационной безопасности среднего бизнеса. Использование сотрудниками различных средств связи, включая мобильные устройства, корпоративные и личные почтовые ящики, облачные сервисы и мессенджеры, создает уязвимости, которые могут быть использованы злоумышленниками для кражи данных, финансового мошенничества или нарушения работы компании. Рассмотрим основные виды киберугроз.

Фишинговые атаки

Фишинг — это один из наиболее распространенных методов кибератак, при котором злоумышленники отправляют сотрудникам компании поддельные электронные письма или сообщения, маскируясь под официальные организации. Основные цели таких атак:

• Получение доступа к учетным записям сотрудников.

• Кража конфиденциальных данных, таких как финансовая информация или корпоративные документы.

• Установка вредоносного ПО на устройства компании.

Пример: Сотруднику приходит электронное письмо якобы от IT-отдела компании с просьбой ввести свои учетные данные для обновления системы безопасности. После ввода логина и пароля информация попадает к злоумышленникам.

2. Вредоносное ПО (малварь)

Вредоносные программы (вирусы, трояны, шпионские программы, программы-вымогатели) могут проникнуть в корпоративную сеть через электронную почту, скачанные файлы или незащищенные устройства сотрудников. Основные последствия заражения:

• Блокировка доступа к данным с требованием выкупа (шифровальщики).

• Кража конфиденциальной информации.

• Незаметное слежение за действиями сотрудников.

*Пример***:** Сотрудник скачал и открыл файл с неизвестного источника, после чего программа-вымогатель зашифровала все файлы на его устройстве и потребовала оплату за их восстановление.

3. Атаки «человек посередине» (Man-in-the-Middle, MITM)

Этот тип атак происходит, когда злоумышленник перехватывает данные, передаваемые между пользователем и сервером, подменяя или анализируя информацию. Это возможно при использовании незащищенных сетей Wi-Fi или слабых каналов связи.

Пример: Сотрудник подключается к общедоступному Wi-Fi в кафе и вводит учетные данные для доступа к корпоративной системе. Хакер, находящийся в той же сети, перехватывает логины и пароли.

4. DDoS-атаки

DDoS (Distributed Denial of Service) — атака, направленная на перегрузку серверов компании путем отправки огромного количества запросов с разных устройств. В результате работа онлайн-сервисов компании нарушается, что приводит к финансовым и репутационным потерям.

Пример: Интернет-магазин подвергается атаке DDoS, и его сайт становится недоступным для клиентов в течение нескольких часов, что приводит к потере прибыли.

5. Внутренние угрозы

Опасность могут представлять не только внешние хакеры, но и сами сотрудники компании, намеренно или случайно создающие угрозы безопасности:

• Использование слабых паролей или их повторное применение.

• Установка неофициального ПО на рабочие устройства.

• Передача корпоративных данных через личные мессенджеры.

Способы защиты от киберугроз

Для минимизации рисков, связанных с киберугрозами, компании должны внедрять комплексные меры безопасности:

• Обучение сотрудников основам кибербезопасности.

• Использование многофакторной аутентификации (2FA) для защиты учетных записей.

• Регулярное обновление программного обеспечения и антивирусных систем.

• Контроль доступа к корпоративным данным и мониторинг подозрительной активности.

Киберугрозы представляют серьезную проблему для субъектов среднего бизнеса. Современные методы атак становятся все более изощренными, что требует от компаний внедрения надежных стратегий киберзащиты, направленных на предотвращение угроз и снижение возможных рисков.

1.2. Утечка данных

Использование личных устройств и незащищенных мессенджеров для передачи корпоративной информации может привести к утечке данных [2]. Нарушение политики безопасности часто происходит из-за человеческого фактора или недостаточного контроля со стороны компании.

2. Методы обеспечения безопасности

2.1. *Разработка политики безопасности*

Компании должны внедрять строгие политики безопасности, регулирующие использование сотрудниками корпоративных и личных средств связи [4].

2.2. *Обучение сотрудников*

Проведение регулярных тренингов по кибербезопасности снижает вероятность человеческих ошибок и повышает уровень защиты информации [5].

2.3. *Использование защищенных каналов связи*

Рекомендуется применять VPN, шифрованные мессенджеры и корпоративные почтовые сервисы с высокой степенью защиты [6].

2.4**.** *Мониторинг и контроль*

Автоматизированные системы мониторинга сетевой активности и управления доступом помогают выявлять подозрительное поведение и предотвращать утечки данных [7].

Заключение

Обеспечение безопасности в среднем бизнесе требует комплексного подхода, включающего технические, организационные и правовые меры. Компании должны разрабатывать и внедрять стратегии защиты информации, минимизируя риски, связанные с использованием сотрудниками средств связи.

Обеспечение безопасности субъектов среднего бизнеса в условиях активного использования сотрудниками средств связи является важной задачей, требующей комплексного подхода. В данной статье рассмотрены основные угрозы, с которыми сталкиваются организации, включая кибератаки, утечки данных, правовые риски и проблемы контроля доступа.

Современные средства связи, такие как мобильные устройства, облачные сервисы и корпоративные мессенджеры, значительно упрощают рабочие процессы, но при этом создают уязвимости, которые могут привести к серьезным финансовым и репутационным потерям. Фишинговые атаки,

вредоносное ПО, атаки «человек посередине» и внутренние угрозы требуют от бизнеса внедрения эффективных стратегий защиты информации.

Для минимизации рисков компаниям необходимо применять комплексные меры, включая разработку четкой политики информационной безопасности, обучение сотрудников кибергигиене, использование защищенных каналов связи, многофакторной аутентификации и систем мониторинга сетевой активности. Кроме того, важно соблюдать требования законодательства о защите персональных данных, чтобы избежать юридических последствий.

Таким образом, безопасность среднего бизнеса в контексте использования средств связи сотрудниками зависит от сочетания технических, организационных и правовых мер. Только интегрированный подход позволит минимизировать угрозы и обеспечить надежную защиту корпоративной информации.

Список использованной литературы

1. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
3. NIST Special Publication 800-53. (2020). Security and Privacy Controls for Federal Information Systems and Organizations.
4. GDPR (General Data Protection Regulation). (2018). Regulation (EU) 2016/679.
5. ISO/IEC 27001:2022. Information security management systems.
6. Kaspersky Lab (2022). Cybersecurity Trends for Business.
7. Symantec Threat Report (2021). Global Cybersecurity Insights.

ҚЫЗМЕТКЕРЛЕРДІҢ БАЙЛАНЫС ҚҰРАЛДАРЫН ПАЙДАЛАНУЫ КЕЗІНДЕ ОРТА БИЗНЕСТІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ

Рахым М.Р. , Шайханова А.К. , Алтынбек С.А.

Бұл мақалада орта бизнес субъектілерінің қауіпсіздігіне қызметкерлердің түрлі байланыс құралдарын пайдалануы нәтижесінде туындайтын негізгі қауіптер қарастырылады. Киберқауіпсіздік мәселелеріне, деректердің сыртқа шығу қатеріне және ақпаратты қорғаудың құқықтық аспектілеріне ерекше назар аударылады. Корпоративтік деректерді қорғаудың заманауи әдістері талданып, қауіптерді азайту бойынша ұсыныстар әзірленеді.

Кілт сөздер: Киберқауіпсіздік, деректердің сыртқа шығуы, орта бизнес, ақпараттық қауіпсіздік, байланыс құралдары, заңнамалық талаптар, корпоративтік деректерді қорғау, шабуылдардан қорғау, ақпараттық технологиялар, қашықтан жұмыс істеу.

ENSURING INFORMATION SECURITY OF MEDIUM-SIZED BUSINESSES WHEN EMPLOYEES USE COMMUNICATION TOOLS

Rakhym M.R., Shaikhanova A.K., Altynbek S.A.

This article examines the main security threats faced by medium-sized businesses due to the use of various communication tools by employees. Particular attention is given to cybersecurity issues, data leakage risks, and legal aspects of information protection. Modern methods of corporate data protection are analyzed, and recommendations for minimizing threats are developed.

Keywords: Cybersecurity, data leakage, medium-sized business, information security, communication tools, legal requirements, corporate data protection, threat prevention, information technology, remote work.

REFERENCES

1. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
3. NIST Special Publication 800-53. (2020). Security and Privacy Controls for Federal Information Systems and Organizations.
4. GDPR (General Data Protection Regulation). (2018). Regulation (EU) 2016/679.
5. ISO/IEC 27001:2022. Information security management systems.
6. Kaspersky Lab (2022). Cybersecurity Trends for Business.
7. Symantec Threat Report (2021). Global Cybersecurity Insights.