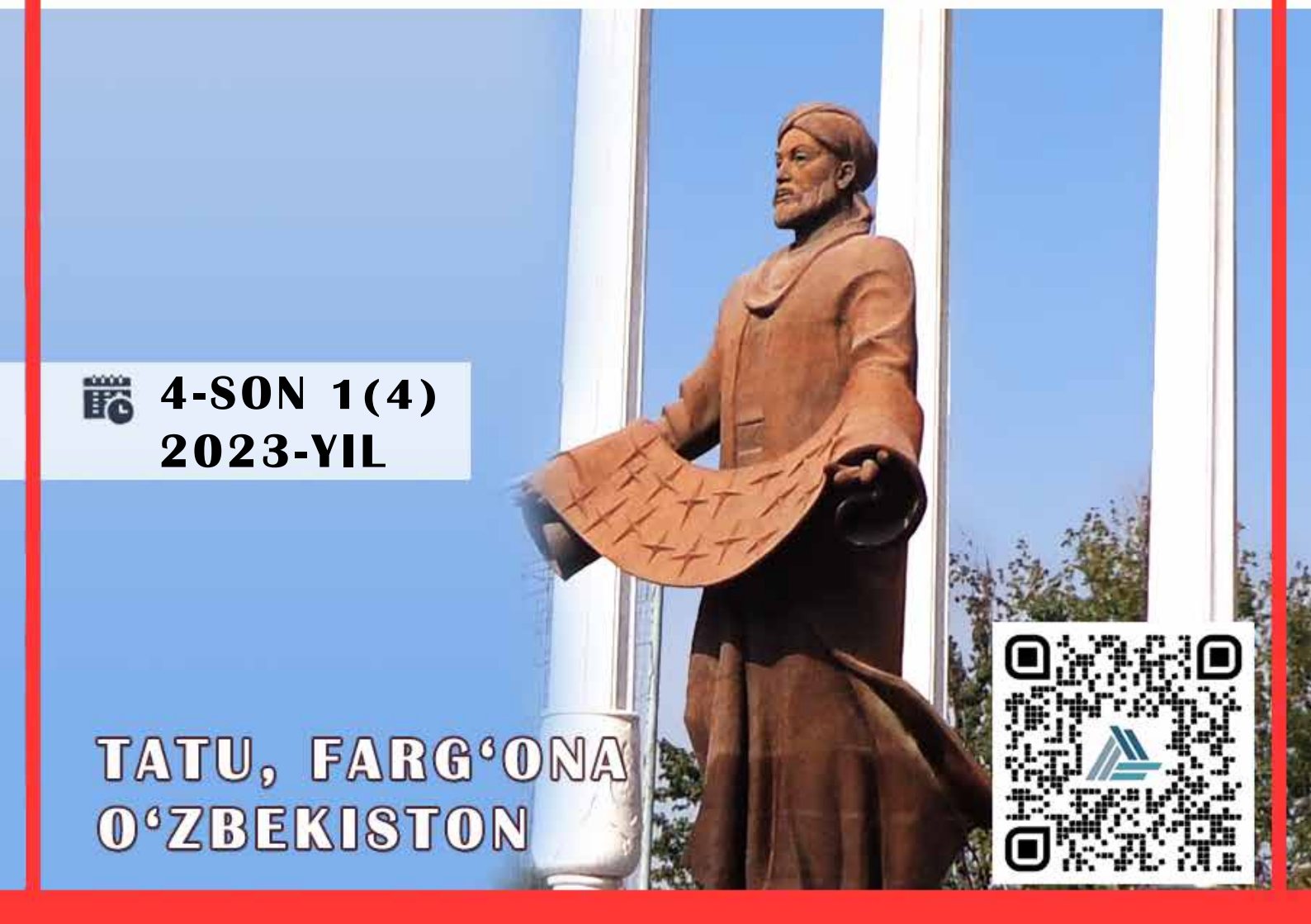
MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI



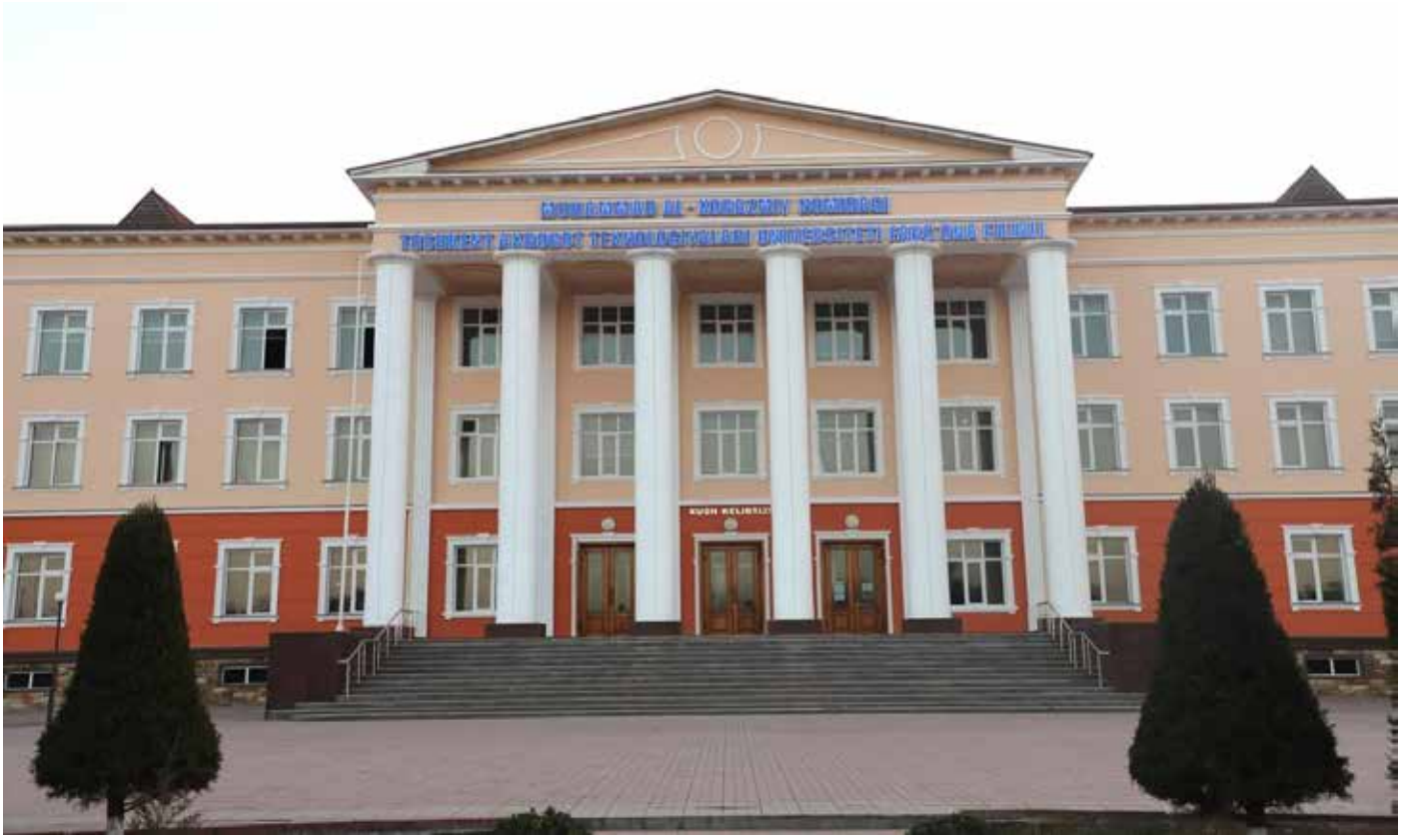
4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI



Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №4
Vol.1, Iss.4, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2023 YIL

Jurnal quyidagi bazalarda indekslanadi:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · DRJI Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОТ КИБЕРАТАК

Хаджаев Саидакбар Исмоил угли,
ассистент кафедры «Программный инжиниринг»
Ферганский филиал ТУИТ имени Мухаммада ал-Хорезми
breddy.bredy@mail.ru

Аннотация: Статья обсуждает актуальность и важность защиты информационных систем малых и средних предприятий в условиях растущих угроз кибербезопасности. Статья выделяет проблемы, с которыми сталкиваются малые и средние предприятия, включая ограниченные ресурсы и уязвимость перед новыми формами кибератак. Обсуждаются важность срочных мер по повышению осведомленности предпринимателей о рисках кибербезопасности, разработке эффективных средств защиты и необходимости сотрудничества с государственными структурами для обеспечения безопасной цифровой среды для малых и средних предприятий. Цель данной статьи заключается в привлечении внимания к актуальной проблеме кибербезопасности малых и средних предприятий и предоставлении основ для разработки и внедрения стратегий защиты информационных систем, способствующих устойчивому развитию и конкурентоспособности малых и средних предприятий в современном цифровом мире.

Ключевые слова: Информационные системы; угрозы кибербезопасности; безопасность данных; цифровая трансформация; осведомленность о рисках; стратегии защиты, кибератаки; малые и средние предприятия(МСП).

Введение. На сегодняшний день, информационные системы являются основой практически всех бизнес-процессов. Малые и средние предприятия активно внедряют цифровые технологии для повышения эффективности, однако, вместе с этим, возрастает уровень угроз для безопасности данных. Злоумышленники постоянно совершенствуют методы атак, и малые компании часто оказываются более уязвимыми из-за ограниченных ресурсов, выделяемых на защиту информации.

В эпоху цифровой трансформации сферы бизнеса, информационные технологии становятся стержнем организационной эффективности, и особенно это актуально для малого и среднего бизнеса (МСБ). Однако, параллельно с ростом важности информационных систем, появляются и усиливаются угрозы кибербезопасности, которые могут оказать разрушительное воздействие на операции и конфиденциальность данных предприятий.

Согласно отчетам исследований в области кибербезопасности, малые и средние предприятия становятся объектами все более изощренных и разнообразных кибератак. Сложность атак существенно возросла, а средства защиты, часто ограниченные ресурсами, не всегда соответствуют новым угрозам. Это создает срочную необходимость в осмысленных и эффективных стратегиях по защите информационных активов МСБ.

В этом контексте, становится ясным, что актуальность проблемы защиты информационных систем малого и среднего бизнеса находится на пике, требуя комплексного подхода к выработке стратегий безопасности и обеспечению устойчивости предприятий в условиях цифровой среды.

Цифровизация современного бизнеса принесла несомненные преимущества, но вместе с этим возросла и угроза кибербезопасности. Малые и средние предприятия, играющие ключевую роль в экономике, стали особенно уязвимыми перед кибератаками. Стремительное развитие технологий предоставило преступникам новые инструменты для вторжения в информационные системы, оставляя МСБ под постоянной угрозой.

Динамичная природа киберугроз требует постоянного обновления и совершенствования мер безопасности. От атаки с использованием вредоносных программ до софтверных уязвимостей, угрозы кибербезопасности проникают в различные слои информационных систем, ставя под угрозу конфиденциальность данных, финансовую устойчивость и репутацию бизнеса.

Имея в виду разнообразие киберугроз, стоит отметить, что предотвращение и защита от атак требуют системного подхода. Это включает в себя не только технические решения, но и стратегическое планирование, обучение персонала, регулярные аудиты безопасности и четкую политику управления доступом.

Однако, многие малые и средние предприятия сталкиваются с вызовом в обеспечении адекватной защиты из-за ограниченных бюджетов или недостаточной осведомленности. Это подчеркивает важность понимания и принятия мер для улучшения кибербезопасности в малых и средних предприятий на всех уровнях.

В нашей статье мы проанализируем эти вызовы и предложим конкретные практические рекомендации, которые могут быть легко внедрены предприятиями любого размера. Мы сфокусируемся на доступных инструментах и методах, а также выделим стратегии, помогающие малым и средним предприятям повысить свой уровень защиты в сфере кибербезопасности. Для МСП также важно внедрять строгую политику доступа к информации. Ограничение доступа к конфиденциальным данным только для авторизованных сотрудников и внешних подрядчиков снижает риск утечки информации или несанкционированного доступа.

Регулярные аудиты безопасности и мониторинг событий в сети также становятся необходимыми для выявления необычной активности или потенциальных угроз в реальном времени. Это поможет оперативно реагировать на возможные инциденты и предотвращать их дальнейшее развитие.

Учитывая нарастающую сложность киберугроз и их потенциальные последствия для бизнеса, важно осознать, что никакая компания не может считать себя неприступной для кибератак. Однако, существуют действенные шаги для улучшения уровня кибербезопасности даже при ограниченных ресурсах.

Важно начать с осознания рисков и уязвимостей в собственной системе. Это требует проведения анализа уязвимостей и оценки рисков, позволяющих выявить слабые места в системе безопасности. Дальше следует разработать стратегию защиты, учитывающую специфику бизнеса, и ориентированную на минимизацию обнаруженных рисков.

Существует ряд технических инструментов и методов, которые могут помочь МСП повысить свой уровень кибербезопасности. Это может быть установка программного обеспечения для защиты от вредоносных программ, регулярное обновление систем и ПО, а также использование межсетевых экранов и шифрования данных.

Однако, помимо технических решений, обучение персонала становится одним из ключевых факторов в защите от киберугроз. Сотрудники играют важную роль в предотвращении атак, поэтому им необходимо обучение по основам безопасности, методам распознавания фишинга и правилам работы с конфиденциальной информацией.

Важно понимать, что кибербезопасность - это не единовременный процесс, а постоянная работа по обеспечению безопасности данных и информационных активов компании. Стремление к непрерывному совершенствованию защиты информации поможет МСП успешно преодолевать угрозы и оставаться устойчивыми в динамичной цифровой среде.

Интеграция мер защиты данных в бизнес-процессы становится важным элементом поддержания кибербезопасности на должном уровне. Это означает включение безопасности во все аспекты развития бизнеса, начиная от планирования до реализации проектов.

В итоге, эффективная защита информационных систем МСП требует комплексного подхода, включающего технические решения, обучение персонала и внедрение строгих политик безопасности. Это позволит бизнесу не только предотвратить потенциальные угрозы, но и

оставаться конкурентоспособным и устойчивым в современной цифровой среде.

Материалы и методы. Методы защиты информационных систем малого и среднего бизнеса требуют комплексного подхода. Эффективная стратегия включает в себя не только технические меры, такие как антивирусное программное обеспечение и фаерволы, но и обучение персонала по вопросам безопасности, регулярное обновление программ и систем, а также регулярные аудиты безопасности.

Статистические данные и отчеты: Обзор статистических данных и отчетов о кибератаках на малые и средние предприятия за последние несколько лет.

Литературный обзор: Анализ актуальных научных статей, публикаций и книг о кибербезопасности малых и средних предприятий, включая лучшие практики и методы защиты.

Исследования и кейс-стади: Изучение случаев кибератак на малые и средние компании, анализ последствий атак на бизнес, включая финансовые и репутационные потери.

Опросы и интервью: Проведение опросов среди предпринимателей и IT-специалистов малых и средних предприятий для оценки осведомленности о кибербезопасности и их методов защиты.

Обзор доступных средств защиты: Сравнительный анализ программного и аппаратного обеспечения, доступного для малых и средних предприятий, с оценкой их эффективности и применимости.

Сбор данных и литературный обзор: Поиск и анализ статистических данных: Использование открытых источников, отчетов о кибератаках на малые и средние предприятия для оценки общей динамики угроз в последние годы.

Литературный обзор и анализ исследований: Изучение актуальных исследований, научных публикаций и отчетов для выявления наиболее актуальных угроз и рекомендаций по защите информационных систем малых и средних предприятий.

Опросы и интервью: Опрос предпринимателей и IT-специалистов: Проведение структурированных опросов для оценки уровня осведомленности о кибербезопасности и понимания текущих методов защиты в малых и средних предприятий.

Интервью с экспертами: Беседы с профессионалами в области кибербезопасности для получения экспертных мнений и рекомендаций по эффективным методам защиты.

Анализ кейсов и исследований: Изучение случаев кибератак на малых и средних предприятий: Анализ конкретных случаев атак и их последствий для выявления основных уязвимостей и путей защиты.

Исследование последствий кибератак: Оценка воздействия атак на бизнес, включая финансовые потери, утечку данных и репутационные риски.

Обзор средств защиты: Сравнительный анализ программных и аппаратных решений: Оценка эффективности доступных инструментов защиты информационных систем малых и средних предприятий, их стоимости и применимости.

Статистический анализ: Обработка и анализ данных: Применение статистических методов для выявления основных тенденций в уровне кибербезопасности малых и средних предприятий, определения наиболее частых угроз и их последствий.

Систематизация информации: Сводка данных и выводы: Обобщение полученной информации для формирования четких выводов о текущей ситуации и основных проблемах в области кибербезопасности для малых и средних предприятий.

Результаты. Исследования показывают, что многие предприятия, особенно в сегменте малого и среднего бизнеса, недооценивают риски, связанные с безопасностью данных. Это приводит к серьезным последствиям, таким как утечки конфиденциальной информации, потери клиентов и повреждение репутации компании. Эффективные меры безопасности могут существенно снизить риски и обеспечить устойчивость бизнеса к цифровым угрозам.

Для малых и средних предприятий (МСП) пренебрежение рисками кибербезопасности оказывается критическим моментом, исходя из результатов исследований. Важно отметить, что это недооценение может привести к многочисленным негативным последствиям,

которые значительно влияют на их функционирование и репутацию.

Утечки конфиденциальной информации оказывают непосредственное воздействие на доверие клиентов. Когда данные о клиентах или коммерческие секреты попадают в несанкционированные руки, это может привести к утрате клиентов, что в свою очередь сказывается на доходах и репутации компании.

Влияние на репутацию - еще одно серьезное последствие. Даже одиночный инцидент безопасности, вроде утечки данных или недоступности сервисов из-за кибератаки, может серьезно подорвать доверие к компании. Репутация, сложившаяся годами, может быть сильно подмочена всего за несколько часов.

Тем не менее, эффективные меры кибербезопасности способны существенно снизить эти риски. Внедрение современных систем защиты, регулярное обновление программного обеспечения, обучение персонала по безопасности и регулярные аудиты безопасности - все это способы, которые могут помочь защитить информационные активы и обеспечить устойчивость бизнеса МСП перед цифровыми угрозами.

На графике можно увидеть процентное соотношение последствия недооценки рисков предприятий.

Последствия недооценки рисков	Процент предприятий
Утечки конфиденциальной информации	30%
Потери клиентов	25%
Повреждение репутации компании	45%

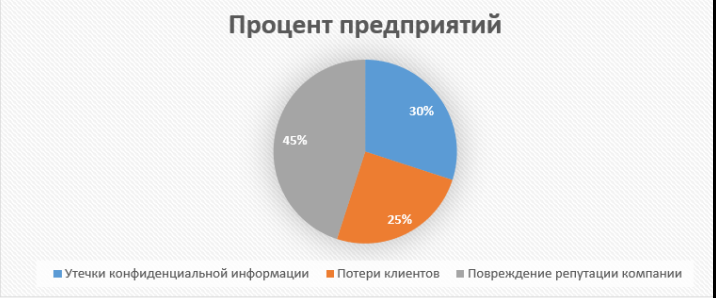


Диаграмма. 1. Последствия недооценки рисков на процентах

Предоставление обширных рекомендаций и образовательных программ по безопасности также имеет критическое значение. Обучение персонала и создание культуры безопасности внутри предприятия помогут снизить риски, связанные с человеческим фактором, который часто является слабым звеном в системах защиты.

Обсуждение

Актуальность проблемы защиты информационных систем малого и среднего бизнеса неоспорима. В современном цифровом мире, где информация — ключевой ресурс, безопасность данных становится приоритетным вопросом для бизнеса любого размера. Комплексный подход, сочетающий технические, организационные и образовательные меры, является необходимым условием успешной защиты информационных систем. Информационная безопасность стала фундаментальным аспектом для устойчивости любого бизнеса в наше время. Малые и средние предприятия (МСП), как двигатели экономики, не могут оставаться в стороне от этой важной проблемы. В сфере кибербезопасности требуется комплексный подход, объединяющий технические инструменты, организационные меры и образовательные программы для защиты информационных систем МСП.

Технические инструменты, такие как межсетевые экраны, антивирусные программы, системы мониторинга и защиты от вторжений, играют важную роль в обеспечении базового уровня защиты. Однако, их эффективность может быть усилена, только если они используются в сочетании с правильными организационными мерами.

Внедрение правильных организационных политик, таких как установление четких правил доступа к информации, управление рисками, регулярное обновление и резервное копирование данных, становится критическим. Но и это не исчерпывает всего спектра необходимых мер.

Образование сотрудников о кибербезопасности также играет важную роль. Человеческий фактор часто является слабым звеном в системе защиты, и обучение сотрудников узнавать и предотвращать угрозы безопасности данных становится необходимостью. Регулярные тренинги и осведомленность о последних трендах в кибербезопасности сокращают риски, связанные с социальной инженерией и фишингом.

Только сочетание всех этих мер позволит МСП эффективно противостоять угрозам кибербезопасности. Актуальность этой проблемы делает ее неотъемлемой частью бизнес-стратегии, и лишь интеграция различных подходов гарантирует защиту информационных систем МСП от постоянно увеличивающегося спектра киберугроз. Только благодаря комплексному подходу к кибербезопасности МСП смогут добиться эффективной защиты информационных активов. Однако, важно осознать, что защита от киберугроз - это постоянный процесс. Угрозы постоянно эволюционируют, и защитные меры также должны развиваться и совершенствоваться.

Безопасность данных становится неотъемлемой частью устойчивости и долгосрочного успеха МСП. Инвестирование в кибербезопасность сегодня - это не только защита от потенциальных угроз, но и инвестиция в доверие клиентов, сохранение репутации и обеспечение бесперебойного функционирования бизнеса.

Сотрудничество с экспертами по кибербезопасности, использование передовых технологий и регулярное обновление методов защиты - все это необходимо для того, чтобы МСП оставались защищенными в динамичной и постоянно меняющейся цифровой среде.

Кибербезопасность для малого и среднего бизнеса - это не только вопрос безопасности данных, но и стратегическое решение, которое влияет на восприятие клиентов, доверие к бренду и долгосрочную стабильность предприятия. Поэтому важно внедрять разносторонние методы защиты, охватывающие технические, организационные и образовательные аспекты.

Технологии играют важную роль, однако только их применение недостаточно для гарантированной защиты. Комплексный подход включает разработку организационных политик, которые регулируют доступ к данным, обновление и резервное копирование информации. Осведомленный и обученный персонал также играет ключевую роль в предотвращении атак, поэтому необходимы регулярные тренинги и обучение по вопросам кибербезопасности. Ниже приведены типы угроз и уровни уязвимостей, возникновения и воздействия их на предприятия.

Тип угрозы	Частота возникновения	Уровень уязвимости	Степень воздействия
Фишинг	Высокая	Средний	Низкий
Вредоносные программы	Средняя	Высокий	Средний
Несанкционированный досту	Низкая	Высокий	Высокий
Атаки на сетевую инфраструктуру	Средняя	Средний	Высокий

Таблица 1. Типы угроз и уязвимостей

Интеграция всех этих мер становится неотъемлемой частью стратегии МСП. Кибербезопасность перестает быть просто "дополнительной опцией", становясь важным элементом, который определяет успех и устойчивость компании в цифровой эпохе. Однако, важно помнить, что защита от киберугроз - это непрерывный процесс, требующий постоянного развития и обновления методов защиты.

Инвестирование в кибербезопасность сегодня - это инвестиция в будущее бизнеса. Партнерство с профессионалами по кибербезопасности, внедрение передовых технологий и регулярное обучение персонала становятся важными шагами для обеспечения надежной защиты данных МСП в динамичном и постоянно меняющемся цифровом мире.

Только осознание актуальности проблемы кибербезопасности и комплексный подход к защите информационных систем помогут МСП эффективно противостоять растущим угрозам в цифровую эпоху и сохранить стабильность и долгосрочный успех в своей деятельности.

В конечном итоге, осознание актуальности проблемы кибербезопасности и принятие соответствующих мер - это ключевой шаг к защите информационных систем МСП и их устойчивости перед возрастающими угрозами в цифровой эпохе.

Заключение. Проблема защиты информационных систем малого и среднего бизнеса требует постоянного внимания и инвестиций. Эффективная стратегия безопасности должна быть встроена в бизнес-процессы, чтобы обеспечить устойчивость компании к цифровым угрозам. Внедрение современных технологий и обучение персонала становятся неотъемлемой частью успешного управления рисками в сфере информационной безопасности малого и среднего

бизнеса. В заключение, защита информационных систем малого и среднего бизнеса - это не просто необходимость, но и стратегическое решение для долгосрочного успеха компании. Эта проблема требует постоянного внимания, инвестиций и систематического подхода.

Встроенная в бизнес-процессы эффективная стратегия безопасности не только обеспечивает защиту данных, но и способствует доверию клиентов, поддерживает репутацию компании и минимизирует потенциальные финансовые потери из-за кибератак.

Важно осознать, что технологии постоянно развиваются, а угрозы кибербезопасности становятся все более сложными и утонченными. Поэтому внедрение передовых технологий и постоянное обучение персонала становятся краеугольными камнями управления рисками в области информационной безопасности для МСП.

Безопасность данных больше не является дополнительной опцией, а становится обязательной составляющей любого бизнеса. Лишь постоянное обновление и улучшение методов защиты данных позволят малым и средним предприятиям оставаться устойчивыми и успешными в цифровой эпохе. Успешная защита информационных систем МСП не только обеспечивает безопасность данных, но и создает основу для инноваций, роста и доверия клиентов. Это также предоставляет возможность дифференцироваться на рынке, демонстрируя готовность брать на себя ответственность за конфиденциальность и целостность информации, что является ключевым фактором в сегодняшнем цифровом мире.

Каждая компания, независимо от размера, должна осознать, что вопросы кибербезопасности не могут быть оставлены на второй план. Они становятся неотъемлемой частью бизнеса и требуют постоянного развития, обучения персонала и инвестиций в современные технологии.

Разработка эффективных стратегий кибербезопасности и их интеграция в основные бизнес-процессы становятся стратегическими шагами для обеспечения конкурентоспособности и устойчивости МСП. Только тогда компании смогут успешно преодолевать вызовы цифровой безопасности и эффективно защищать свои информационные активы в долгосрочной перспективе.

Литература:

[1] Xadjayev S. Information Security: Strategies, Challenges, and Emerging Trends //Journal of technical research and development. – 2023. – Т. 1. – №. 2. – С. 253-257.

[2] "Кибербезопасность: Защита информации в современной организации" авторства Уильяма Сталингса.

[3] Coding the Path to E-Commerce Excellence: A Web Programming Odyssey. (2023). Journal of Technical Research and Development, 1(2), 471-475. https://jtrd.mcdir.me/index.php/jtrd/article/view/101

[4] Uzbekistan’s Digital Market: Python’s E-Commerce Impact. (2023). Journal of Technical Research and Development, 1(1), 58-61. https://jtrd.mcdir.me/index.php/jtrd/article/view/5

[5] Исследования, проведенные Консорциумом по кибербезопасности для малых и средних предприятий (National Cyber Security Consortium for Small and Midsize Businesses).

[6] Saidakbar X. USING MODERN WEB TECHNOLOGIES IN CREATING WEB APPLICATIONS //Journal of technical research and development. – 2023. – Т. 1. – №. 2.