УДК 658.012.32:004.056

КИБЕРБЕЗОПАСНОСТЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БИЗНЕСОМ

Ананич А. Д., студент,
Савицкая Е. В., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: магистр техн. наук старший преподаватель Петровская Т. А.

Аннотация. В данной статье рассмотрим, что собой представляет кибербезопасность в информационных системах управления бизнесом. Проанализируем ключевые инструменты безопасности – от обучения сотрудников и фильтрации трафика до регулярных обновлений и контроля доступа.

Кибербезопасность – это практика защиты систем, сетей и данных от любых форм цифровых атак. Целью этих атак обычно является доступ к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег с помощью программ-вымогателей или нарушение повседневных бизнес-процессов. с ростом числа устройств и уровня подключения к Интернету растут и связанные с ними риски. Поэтому внедрение мер кибербезопасности стало необходимостью для предотвращения подобных вторжений и обеспечения безопасности ваших данных [1].

Кибербезопасность защищает бизнес-данные и информацию о клиентах, которые являются ключевыми факторами бесперебойной работы бизнеса. Неотъемлемыми элементы кибербезопасности для бизнеса являются:

1. Резервное копирование данных: регулярно создавайте резервные копии критически важных данных и систем, чтобы в случае атаки, например, программ-вымогателей, можно было восстановить информацию.

2. Шифрование данных: Используйте шифрование для защиты конфиденциальных данных как в покое, так и в движении, что поможет предотвратить доступ к ним со стороны злоумышленников.

3. Многофакторная аутентификация (MFA): внедрите многофакторную аутентификацию для всех учетных записей, чтобы повысить безопасность при входе в систему и снизить вероятность несанкционированного доступа.

4. Политики безопасности: Разработайте и внедрите четкие политики безопасности, которые будут описывать допустимые действия сотрудников с информацией и технологиями.

5. Мониторинг и аудит: Осуществляйте постоянный мониторинг сетевой активности и проводите регулярные аудиты безопасности для выявления и устранения уязвимостей.

6. Учебные симуляции: проводите регулярные симуляции кибератак или фишинговых угроз, чтобы подготовить сотрудников к действию в случае реальной угрозы.

7. Обновления антивируса и вредоносного ПО: регулярно обновляйте антивирусное и вредоносное ПО, чтобы защитить себя от новых угроз [1].

Кибербезопасность важна для бизнеса, поскольку кибератаки могут иметь серьезные последствия, такие как финансовые потери, ущерб репутации и сбои в работе.

Для бизнеса кибербезопасность подразумевает защиту не только собственных активов компании, но и данных и другой конфиденциальной информации ее клиентов.
В этом смысле кибербезопасность функционирует через многоуровневую систему защиты, включающую людей, процессы и технологии.

Люди – должны быть обучены выявлять попытки фишинга, использовать надежные пароли и следовать протоколам безопасности высокого уровня.

Процессы – компании должны иметь структурированные планы по выявлению, защите и восстановлению после кибератак.

Технологии – использование брандмауэров, антивирусного программного обеспечения и шифрования для защиты устройств, сетей и облачных систем [2].

Для того чтобы защитить свой бизнес от киберпреступности необходимо изучить свои данные, определяя тип и объем данных, с которыми работает ваша компания, чтобы точно оценить ее потребности в безопасности. Регулярно выполняйте резервное копирование, убеждаясь, что все важные данные и файлы регулярно резервируются на защищенном сервере на случай потенциальной утечки. Предоставьте доступ к конфиденциальным данным только необходимому персоналу. Это снизит риск разглашения. Обучайте персонал распознавать попытки фишинга и социальной инженерии, тем самым укрепляя первую линию защиты от таких нарушений. Проверка биографических данных сотрудников поможет снизить внутренние угрозы. Поддерживайте актуальность программного обеспечения; необходимо периодически обновлять системное ПО. Устанавливайте свежие исправления безопасности и самые последние версии программного обеспечения. Инвестиции в цифровую безопасность приносят бизнесу множество преимуществ: от снижения вероятности утечек данных и успешных кибератак до создания репутации надежного и безопасного поставщика.

Соблюдение нормативных требований позволит избежать риска манипуляций и штрафов. А чрезвычайные меры помогают предотвращать проблемы, связанные с бизнес-процессами, и связанные с ними атаки на сеть. Таким образом, цифровая безопасность крайне важна для любого бизнеса любого размера: в условиях постоянно растущего уровня киберугроз внедрение эффективных мер кибербезопасности для обеспечения безопасности бизнеса становится необходимостью. Будь то защита конфиденциальной информации или обеспечение непрерывности работы, инвестиции в кибербезопасность гарантируют долгосрочный успех бизнеса. Поэтому, если вы хотите укрепить безопасность своего бизнеса, рассмотрите такие варианты, как бизнес-кредит, для финансирования необходимых улучшений.

В заключение следует отметить, что кибербезопасность жизненно важна для компаний любого типа и размера. В связи с ростом киберпреступности компаниям необходимо принимать эффективные меры безопасности для защиты своих активов и данных. Будь то защита конфиденциальной информации или обеспечение непрерывности работы, инвестиции в кибербезопасность гарантируют долгосрочный успех бизнеса.

Список использованных источников

1. Роль владельца бизнеса в обеспечении кибербезопасности: делегировать нельзя контролировать. – URL: https://www.nic.ru/help/rol6-vladel6ca-biznesa-v-obespechenii-kiberbezopasnostidelegirovat6nel6zyakontrolirovat6_14075.html?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 28.11.2025).

2. Ларионова, Н. Кибербезопасность в бизнесе – игнорировать нельзя использовать / Н. Ларионова. – URL: https://incrussia.ru/understand/kiberbezopasnost-v-biznese-riski/ (дата обращения: 28.11.2025).