УДК 004.02

Вегера М. Р.
студент 2-го курса,
Дашкевич Т. В.
ст. преп.
Брестский государственный технический университет, г. Брест, Беларусь

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ МАЛЫХ БИЗНЕСОВ

Киберугрозы стали глобальной проблемой для компаний различных размеров, особенно для малого бизнеса. Исследования подтверждают, что небольшие фирмы особенно уязвимы к кибератакам из-за недостатка ресурсов для обеспечения надежной защиты. Обеспечение кибербезопасности критически важно для любого бизнеса, но быстро меняющийся характер угроз затрудняет определение приоритетов и первых шагов. Кибератаки могут привести к таким последствиям, как потеря данных, повреждение оборудования и серьезные финансовые убытки.

Злоумышленники имеют возможность получить доступ к конфиденциальной информации, такой как списки клиентов, данные банковских карт, финансовые реквизиты компании, ценовая политика, интеллектуальная собственность и использовать её в своих целях [1].

В эпоху всеобщего распространения удаленной работы вопросы кибербезопасности становятся критически важными. Значительное число малых предприятий регулярно применяют облачные сервисы и онлайн-инструменты для организации встреч, маркетинговых кампаний, закупки товаров, продаж, коммуникации с клиентами и партнерами, а также проведения финансовых транзакций. Для предотвращения серьезных финансовых и репутационных потерь, крайне важно обеспечить надежную защиту данных и облачных платформ от неавторизованного проникновения и утечек информации.

Вот ключевые рекомендации по защите от киберугроз [1]:

1. Обучение персонала. Следует проводить регулярные тренинги по кибербезопасности и научить сотрудников созданию надежных паролей и распознаванию фишинга, разработать четкие политики работы с данными.

2. Оценка рисков. Следует проанализировать, где хранятся данные, и кто имеет к ним доступ, разработать план устранения уязвимостей и регулярно обновлять стратегию безопасности.

3. Позаботьтесь о технической защите, используйте современное антивирусное программное обеспечение. Внедрите шифрование конфиденциальной информации, защитите Wi-Fi сеть сложным паролем и обеспечьте сотрудников VPN для безопасной удаленной работы.

4. Управление доступом. Ограничьте доступ к важным данным, сделайте его доступным только для необходимых сотрудников. Внедрите политику сложных паролей (минимум 10 символов). Также попрактикуйте регулярную смену паролей, тем самым вы повысите уровень защиты.

5. Защита мобильных устройств, обязательное установление паролей и скачивание защитных(антивирусных) приложений. Разработайте протокол действий при утере мобильных устройств.

6. Работая со сторонними компаниями, проверяйте их уровень кибербезопасности и убедитесь в соблюдении схожих стандартов защиты.

Следуя этим рекомендациям, вы существенно повысите уровень защиты вашего бизнеса от киберугроз.

Но если вдруг вы столкнулись с киберугрозой, важно действовать быстро и последовательно [2]:

1. Сразу же смените пароли ко всем аккаунтам, отключите устройство от интернета.

2. Свяжитесь со службой поддержки банков и онлайн-сервисов, обратитесь в полицию и предоставьте все имеющиеся данные, сообщите близким, чтобы они были начеку.

3. Просканируйте устройства антивирусом, восстановите данные из резервных копий, при необходимости обратитесь к специалистам по кибербезопасности.

4.Создайте новые надежные пароли и регулярно делайте резервные копии важных данных [3].

Малому бизнесу необходимо осознать важность кибербезопасности и предпринять необходимые шаги для защиты своих активов и данных. В противном случае, они рискуют стать жертвами киберпреступников и понести непоправимый ущерб [2]. Внедрение продуманной стратегии кибербезопасности — это не просто хорошая практика, а необходимое условие для долгосрочного процветания и устойчивости малого бизнеса в современном цифровом мире.

Помните, что ваша безопасность в интернете зависит от ваших действий. Лучше потратить время на предотвращение угроз, чем разбираться с их последствиями.

Список источник

1. Защита малого бизнеса от киберугроз [Электронный ресурс] // kaspersky : [сайт]. [2025]. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-cyber-security (дата обращения: 06.04.2025).

2. Кибербезопасность [Электронный ресурс] // Википедия : [сайт]. [2025]. URL : https://ru.wikipedia.org (дата обращения: 06.04.2025).

3. Интернет безопасность [Электронный ресурс] // Википедия : [сайт]. [2025]. URL: https://ru.wikipedia.org/ (дата обращения: 06.04.2025).