УДК 004.056

Мельничук Д. А.
к.э.н., доц.,
Фоменко В. О.
студент,
Горлова Е. Д.
студент
Донбасский государственный технический университет, г. Алчевск, ЛНР, Россия

КИБЕРБЕЗОПАСНОСТЬ И РИСКИ ЦИФРОВИЗАЦИИ ДЛЯ УПРАВЛЕНИЯ

На данном этапе человечество проживает расцвет информационного века. В условиях цифровизации кибербезопасность обретает все большее значение. С развитием информационных технологий и цифровых платформ управление компаниями и организациями становится удобным, эффективным и гибким, что обуславливается автоматизацией большинства бизнес-процессов, экономией ресурсов и др. Однако это, в свою очередь, привносит свои риски и угрозы, связанные с кибератаками, утечкой конфиденциальной информации и другими киберугрозами.

Цель исследования — анализ цифровых рисков и кибербезопасности в современной экономике; рассмотрение способов защиты информации в современном мире.

Кибербезопасность представляет собой область знаний и практики, занимающейся защитой компьютерных систем, сетей, данных от несанкционированного доступа, уничтожения, фальсификации или утечки информации [1]. Этот термин подразумевает собой совокупность мер и технологий, предотвращающих кибератаки, а также обнаруживающих подобные атаки на ранних стадиях и сводящих к минимуму их последствия. Задача кибербезопасности заключается в обеспечении безопасности информации путем защиты информационных систем и конфиденциальной информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения.

Специалисты по обеспечению безопасности информации и систем в рамках кибербезопасности выполняют следующие функции: мониторинг и анализ факторов угрозы в киберпространстве и создание политики и процедур информационной безопасности.

Мониторинг и анализ факторов угрозы в киберпространстве входит в категорию специализации работников кибербезопасности. Специалист этого направления рассматривает виды атак, уязвимости систем, а впоследствии разрабатывает стратегии по предотвращению и реагированию на соответственные угрозы. Создание политики и процедур информационной безопасности прямая обязанность эксперта по информационной безопасности в организации. Эксперт изучает уязвимость систем, разрабатывает и устанавливает меры безопасности при управлении доступом к информации, следит за соблюдением требований законодательства и конфиденциальности.

Эксперты кибербезопасности проводят тренинги по основам данной области для начинающих пользователей. В процессе обучения специалисты создают информационные материалы, организовывают тренинги и проводят профилактические мероприятия для повышения осведомленности людей в сфере безопасности. Пользователи, в свою очередь, принимают меры по защите своих данных, а также соблюдают данные меры.

Рассмотрим существующие функции киберзащиты. Каждая из них выполняет основную часть в обеспечении безопасности информации и систем. Их сочетание помогает создать надежную оппозицию опасностям в киберпространстве:

– идентификация и аутентификация пользователей. Сюда входит установление личности и прав доступа пользователей к информационным ресурсам;

– мониторинг и обнаружение угроз включают постоянное отслеживание сетевого трафика и системных ресурсов для выявления потенциальных атак;

– защита от вредоносного программного обеспечения. Обеспечение защиты от вирусов, шпионского программного обеспечения и других видов вредоносных программ;

– реагирование на инциденты. Оперативное реагирование на кибератаки, восстановление систем после инцидента и проведение расследования;

– обучение и осведомленность пользователей подразумевает проведение обучающих мероприятий для сотрудников по правилам безопасности информации;

– управление доступом. Контроль доступа пользователей к конфиденциальной информации и ограничение прав доступа в соответствии с принципом наименьших привилегий;

– шифрование данных. Защита конфиденциальной информации путем шифрования данных в хранении и передаче;

– аудит безопасности. Проведение регулярного аудита систем безопасности для выявления слабых мест и улучшения уровня защиты;

– соблюдение законодательства. Обеспечение соблюдения требований законодательства в области киберзащиты, включая защиту персональных данных и конфиденциальной информации.

Защита цифровой информации и обеспечение кибербезопасности играют важную роль в современном бизнесе, особенно в условиях активной цифровизации процессов управления [2]. Риск кибератак непредсказуем и, тем самым, может нанести серьезный ущерб деятельности компании. Поэтому разработка комплексной стратегии безопасности, аудит систем безопасности, обучение персонала и регулярное обновление защитных мер являются обязательными для любой компании. Используя новейшие технологии и применяя проактивный подход к обнаружению и предотвращению угроз, можно управлять рисками цифровизации и обеспечивать защиту информации в компании.

Эффективная защита цифровой информации также требует регулярного мониторинга и анализа уязвимостей, внедрения антивирусного и антифишингового программного обеспечения, использования шифрования данных и многофакторной аутентификации. Также важно регулярно создавать резервные копии данных и тестировать системы безопасности, чтобы убедиться в их эффективности. Кроме того, важную роль в защите информации играет постоянное знакомство с последними тенденциями и методами атак в мире кибербезопасности.

Кроме того, для эффективной киберзащиты необходимо регулярно обучать сотрудников компании кибергигиене: учить создавать сложные и уникальные пароли для своих учетных записей, поощрять использование многофакторной аутентификации для защиты учетных записей, проверять настройку антивирусной программы, регулярно обновлять программное обеспечение, соблюдать осторожность в сети и создавать регулярные резервные копии документации.

Список источников

1. Ашманов И. С., Касперская Н. И. Цифровая гигиена. СПб. : Питер, 2022. 508 с.

2. Грачева Ю. В. Риски цифровизации. Виды, характеристика, уголовно-правовая оценка. М. : Проспект, 2022. 272 с.