УДК 004.056.53

КИБЕРБЕЗОПАСНОСТЬ: ОСНОВНЫЕ УГРОЗЫ И СПОСОБЫ ИХ МИНИМИЗАЦИИ

Костенко А. А.
Научный руководитель – ст. преподаватель Главницкая И. Н.
Белорусский национальный технический университет,
glavnitskaya@mail.ru

Аннотация. В современном мире, где технологии проникают в каждый аспект нашей жизни, кибербезопасность становится все более важной. Она охватывает практики защиты компьютерных систем, сетей и данных от цифровых атак.

Правовые аспекты кибербезопасности включают законы, нормативы и акты законодательства, которые регулируют эту область и обеспечивают защиту как для индивидов, так и для организаций.

Ключевые слова: кибербезопасность, защита, данные, нарушение, последствие

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [1].

Включает в себя технологии, процессы и контрольные механизмы, которые помогают защитить системы, сети, программы, устройства и данные от кибератак. Кроме того, она включает в себя стратегии риска, которые помогают организациям понять и управлять потенциальными рисками для их цифровых ресурсов. Осуществляя меры кибербезопасности, можно защититься от атак, которые имеют целью доступ к информации, изменение или уничтожение чувствительной информации, вымогательство денег у пользователей, нарушение нормальных бизнес-процессов.

Среди многочисленных угроз кибербезопасности особенно выделяются:

вирусы и вредоносное ПО: программы, предназначенные для нанесения ущерба или несанкционированного доступа;

фишинг и социальная инженерия: методы обмана, направленные на получение конфиденциальной информации;

атаки на критически важную инфраструктуру: направлены на дестабилизацию функционирования государственных и частных систем;

кибершпионаж и кибервойны: использование киберпространства для разведывательной деятельности и военных целей.

Для Республики Беларусь наиболее характерен такой метод хищения денежных средств субъектов хозяйствования как «фишинг».

Обнаружить попытку фишинговой атаки не сложно, если обладать базовой компьютерной грамотностью и уделять должное внимание анализу и проверке писем, посещаемых сайтов и веб-страниц. Необходимо обращать

внимание на URL-адрес ресурса, поскольку при фишинге адрес отличается на 1–2 буквы, цифры или 1–2 символа. Получая электронные письма, следует проанализировать не только содержимое, но и отправляемое [2].

Последствия нарушения кибербезопасности могут быть серьезными и многообразными. Рассмотрим некоторые из них.

1. Юридические последствия.

Нарушение законов о кибербезопасности может привести к административной ответственности, уголовному преследованию и даже международным санкциям. Например, Общий регламент по защите данных (GDPR) в Европейском Союзе, предусматривает строгие штрафы за нарушение правил защиты данных.

2. Финансовые последствия.

Штрафы и компенсации за нарушение кибербезопасности могут достигать значительных сумм, особенно в случаях крупных утечек данных.

Организации также могут столкнуться с потерями из-за утечки конфиденциальной информации, включая затраты на восстановление систем и данных.

3. Репутационные риски.

Нарушения могут привести к потере доверия клиентов и партнеров, что отрицательно скажется на доходах и бизнес-отношениях.

Ущерб репутации может иметь долгосрочные последствия для рыночной стоимости организации.

4. Юридические последствия для отдельных лиц.

Физические лица могут столкнуться с уголовной и административной ответственностью, включая штрафы и лишение свободы.

Гражданские иски могут быть поданы пострадавшими сторонами в случае ущерба их интересам или нарушения их прав.

Уголовный кодекс Республики Беларусь содержит ряд статей, которые предусматривают уголовную ответственность за киберпреступность:

– ст.212 «Хищение путем использования компьютерной техники»;

– ст.349 «Несанкционированный доступ к компьютерной информации»;

– ст.350 «Модификация компьютерной информации»;

– ст.351 «Компьютерный саботаж»;

– ст.352 «Неправомерное завладение компьютерной информацией»;

– ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;

– ст.354 «Разработка, использование либо распространение вредоносных программ»;

– ст.355 «Нарушение правил эксплуатации компьютерной системы или сети» [3].

Эти последствия подчеркивают важность соблюдения законодательства и принятия мер по обеспечению кибербезопасности.

Среди проблем и вызовов в области кибербезопасности можно выделить:

– быстрое развитие технологий: законодательство часто не успевает за технологическим прогрессом;

– международное сотрудничество: сложности согласования действий на международном уровне;

– защита персональных данных: баланс между безопасностью и приватностью.

Для минимизации рисков в области кибербезопасности необходим комплексный подход, включающий следующие меры.

1. Обеспечение соответствия законодательству.

Регулярное обновление политики безопасности и соблюдение нормативно-правовых требований помогают предотвратить юридические последствия и финансовые потери.

Важно следить за изменениями в законодательстве и адаптировать внутренние процедуры для их соответствия.

2. Технические меры.

Использование современных систем защиты информации, таких как шифрование данных и многофакторная аутентификация, повышает уровень безопасности.

Регулярное обновление программного обеспечения и использование надежных антивирусных решений защищают от вредоносных атак.

3. Обучение персонала.

Проведение регулярных тренингов по кибербезопасности и формирование культуры безопасности среди сотрудников снижает риск человеческого фактора.

Важно обучать сотрудников распознаванию фишинговых атак и других видов социальной инженерии.

4. Сотрудничество с правоохранительными и иными государственными органами.

Сотрудничество с правоохранительными и регулирующими органами позволяет оперативно реагировать на угрозы и обмениваться информацией о новых видах атак.

Участие в отраслевых и международных программах по кибербезопасности укрепляет общую безопасность.

5. Регулярный аудит и тестирование систем.

Проведение регулярных аудитов и тестирований помогает выявлять уязвимости и устранять их до того, как они будут использованы злоумышленниками.

Анализ инцидентов нарушений кибербезопасности и усовершенствование систем на основе полученных данных способствует повышению уровня защиты.

6. Разработка плана реагирования на инциденты нарушения кибербезопасности.

Наличие четко определенного плана действий в случае кибератаки позволяет быстро и эффективно реагировать, минимизируя потери.

Регулярные учения и тренировки по реагированию на инциденты повышают готовность персонала и систем к реальным угрозам.

Эти меры должны быть интегрированы в общую стратегию кибербезопасности организации и постоянно совершенствоваться в соответствии с развитием технологий и изменением угроз.

Закон Республики Беларусь от 10 ноября 2008 г. «О информации, информатизации и защите информации» [4] устанавливает правовые основы обработки информации и ее защиты. На практике этот закон направлен на борьбу с киберпреступностью и защиту информационной инфраструктуры. Анализ судебных дел и статистики может помочь оценить его реальное влияние на уровень кибербезопасности в стране.

Согласно Указу Президента Республики Беларусь № 40 от 14.02.2023 г. создана национальная система обеспечения кибербезопасности [5].

Важным аспектом является разработка и внедрение стандартов и процедур для защиты критически важных отраслей, таких как энергетика, транспорт и финансы. Это включает в себя обучение персонала, аудиты безопасности и реагирование на инциденты.

Республика Беларусь участвует в международных инициативах и соглашениях, направленных на укрепление кибербезопасности. Это сотрудничество может включать обмен информацией о угрозах, совместные учения и координацию в борьбе с киберпреступностью.

Полагаем, кибербезопасность – это не просто техническая задача, но и социальная, экономическая и политическая проблема, которая требует совместных усилий всех участников общества: от индивидуальных пользователей до государственных органов.

Законодательство Республики Беларусь в области кибербезопасности играет ключевую роль в создании безопасного цифрового пространства и помогает предотвратить киберпреступления, защитить основные права и свободы граждан и организаций в интерне-пространстве.

Список использованных источников:

1. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» [Электронный ресурс]. – Режим доступа: https://security.beltelecom.by/2021/12/30/ sovremennie_aspekti_kiberbezopasnosti/. – Дата доступа: 15.03.2024.

2. Современные аспекты кибербезопасности [Электронный ресурс]. – Режим доступа: https://security.beltelecom.by/2021/12/30/sovremennie_aspekti_kiberbezopasnosti/. – Дата доступа: 17.03.2024.

3. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=hk9900275. – Дата доступа: 17.03.2024.

4. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=h10800455. – Дата доступа: 15.03.2024.

5. Указ президента Республики Беларусь № 40 от 14.02.2023 г. «О кибербезопасности» [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g. – Дата доступа: 17.03.2024.