﻿Научная статья Original article УДК 004.424

**РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ**

DEVELOPMENT OF AN ORGANIZATION’S SECURITY POLICY

**Горбачев Никита Эдуардович,** студент, Казанский национальный исследовательский технологический университет, г. Казань (420015 Россия г. Казань, ул. Карла Маркса 68), [mineman0228@gmail.com](mailto:mineman0228@gmail.com)

**Алексеева Анна Александровна,** доцент, Казанский национальный исследовательский технологический университет, г. Казань (420015 Россия г. Казань, ул. Карла Маркса 68), [annank90@mail.ru](mailto:annank90@mail.ru)

**Gorbachev Nikita Eduardovich,** student, Kazan National Research Technological University, Kazan (420015 Russia Kazan, Karl Marx 68), [mineman0228@gmail.com](mailto:mineman0228@gmail.com)

**Alekseeva Anna Alexandrovna,** docent, Kazan National Research Technological University, Kazan (420015 Russia Kazan, Karl Marx 68), [annank90@mail.ru](mailto:annank90@mail.ru)

Введение

Политика безопасности организации — это набор правил, процедур и инструкций, которые определяют, как организация защищает свои информационные ресурсы от угроз и рисков.

Разработка политики безопасности является важным этапом в создании системы защиты информации на предприятии.

Наличие политики безопасности помогает предотвратить утечку конфиденциальной информации, снизить риски финансовых потерь и сохранить репутацию компании.

Целью статьи является анализ и разработка рекомендации для реализации успешной политики безопасности организации.

**Основные элементы политики безопасности**

Для начала рассмотрим основные элементы политики безопасности. К ним относятся физическая и информационная безопасность, а также безопасность персонала.

Физическая безопасность — это комплекс мер, направленных на защиту людей, имущества и информации от физических угроз, таких как кражи, взломы, пожары, наводнения и другие стихийные бедствия.

**Основные принципы физической безопасности:**

1. Защита от краж и взломов — установка систем видеонаблюдения, сигнализации, замков и других средств защиты.

2. Защита от пожаров и других стихийных бедствий — установка систем пожарной сигнализации, пожаротушения, дымоудаления и других средств защиты.

3. Контроль доступа — установка систем контроля доступа, таких как электронные замки, биометрические системы и другие средства, которые позволяют контролировать доступ к определенным помещениям и объектам.

Для обеспечения физической безопасности используются различные методы и технологии, такие как системы видеонаблюдения, сигнализации, системы контроля доступа, системы пожарной сигнализации и пожаротушения, а также обучение персонала правилам безопасности.

**Основные принципы информационной безопасности:**

1. Конфиденциальность — защита информации от несанкционированного доступа.

2. Целостность — обеспечение точности и полноты информации.

3. Доступность — обеспечение возможности использования информации по назначению.

Для обеспечения информационной безопасности используются различные методы и технологии, такие как шифрование данных, аутентификация пользователей, контроль доступа, антивирусные программы, системы обнаружения вторжений и другие.

**Основные принципы безопасности персонала:**

1. Предотвращение несчастных случаев — разработка и внедрение мер, направленных на предотвращение травм и заболеваний на рабочем месте.

2. Обеспечение безопасных условий труда — создание условий, при которых работники могут выполнять свои обязанности без риска для здоровья и жизни.

3. Соблюдение правил техники безопасности — обучение работников правилам техники безопасности и контроль за их соблюдением.

Для обеспечения безопасности персонала используются различные методы и технологии, такие как обучение работников правилам техники безопасности, использование средств индивидуальной защиты, проведение регулярных проверок и аудитов безопасности, а также разработка и внедрение систем управления безопасностью труда.

Чтобы создать успешную политику безопасности, необходимо знать, какие этапы включает в себя разработка политики безопасности.

**Этапы разработки политики безопасности**

1. Анализ рисков — определение угроз и рисков, связанных с информационной безопасностью, а также оценка их вероятности и последствий.

2. Определение целей — определение целей и задач политики безопасности, а также определение того, какие меры должны быть приняты для достижения этих целей.

3. Разработка политики — разработка документа, который содержит основные принципы и правила информационной безопасности, а также определяет ответственность и обязанности каждого сотрудника в области информационной безопасности.

4. Внедрение политики — внедрение разработанной политики безопасности в организации, включая обучение персонала, установку необходимого программного и аппаратного обеспечения, а также контроль за соблюдением политики.

5. Мониторинг и аудит — постоянный мониторинг и аудит системы информационной безопасности для выявления возможных уязвимостей и нарушений политики безопасности.

Важно отметить, что разработка политики безопасности должна быть основана на реальных потребностях организации и учитывать ее специфику. Кроме того, политика безопасности должна регулярно обновляться и адаптироваться к изменяющимся условиям и угрозам.

Примеры реализации политики безопасности крупными компаниями показывают, насколько важен серьезный подход к этапам разработки политики безопасности.

**Примеры реализации политики безопасности**

Одним примером организации с успешной политикой безопасности является компания Apple. Apple также известна своими строгими мерами безопасности, которые помогают защитить данные пользователей и корпоративную информацию.

Компания использует многоуровневую систему безопасности, которая включает в себя шифрование данных, двухфакторную аутентификацию, мониторинг активности пользователей и другие меры. Кроме того, Apple активно работает над улучшением своих систем безопасности, регулярно обновляет программное обеспечение и проводит обучение сотрудников по вопросам безопасности.

Эти меры помогли Apple избежать многих серьезных уязвимостей и предотвратить утечки данных. Компания также активно сотрудничает с исследователями безопасности, чтобы обнаруживать и устранять уязвимости в своих продуктах.

Один из примеров организации с неудачной политикой безопасности - это компания Target, которая стала жертвой одной из крупнейших утечек данных в истории США в 2013 году.

В декабре 2013 года злоумышленники взломали систему безопасности компании Target и получили доступ к личным данным миллионов клиентов, включая номера кредитных и дебетовых карт, адреса электронной почты и другую конфиденциальную информацию.

Основной причиной этой утечки данных стала слабая политика безопасности компании. Target не обновляла свои системы безопасности в течение длительного времени, что позволило злоумышленникам использовать уязвимости в системе для получения доступа к данным клиентов.

Последствия этой утечки были серьезными: компания потеряла доверие клиентов, ее акции упали, а также были наложены штрафы и санкции со стороны регулирующих органов.

Этот пример показывает, что даже крупные и успешные компании могут стать жертвами хакерских атак, если не уделяют должного внимания безопасности своих систем и данных.

Одним из примеров успешной реализации политики безопасности среди российских компаний является Сбербанк. Компания активно работает над защитой своих клиентов от киберугроз и мошенничества. В рамках этой работы Сбербанк использует передовые технологии для обнаружения и предотвращения кибератак, проводит регулярные тренинги для сотрудников по вопросам информационной безопасности, а также информирует клиентов о возможных угрозах и способах защиты от них. Благодаря этим мерам, Сбербанк смог значительно снизить уровень киберпреступлений и защитить своих клиентов от финансовых потерь.

Одним из примеров провальной реализации политики безопасности среди российских компаний является случай с компанией «Ортека». В начале марта 2024 года стало известно о том, что ИТ-инфраструктура сети ортопедических салонов «Ортека» (orteka.ru) подверглась хакерской атаке. Полная база данных содержит информацию о покупателях: это имя и фамилия, адрес доставки, хешированный пароль, пол и пр. Кроме того, дамп включает сведения о заказах и картах лояльности — приблизительно 3,8 млн уникальных номеров телефонов и 428 тыс. уникальных адресов электронной почты.

**Заключение**

На основании представленных данных можно сделать вывод, что создание эффективной политики безопасности — это важный шаг для любой организации, которая хочет защитить свои данные и инфраструктуру от кибератак и других угроз. Анализ литературы позволил сформулировать некоторые рекомендации, которые помогут создать эффективную политику безопасности:

1. Определите цели и задачи политики безопасности.

2. Определите риски и угрозы, с которыми может столкнуться ваша организация.

3. Разработайте план действий в случае возникновения инцидента безопасности.

4. Установите правила доступа к данным и ресурсам компании.

5. Обучите сотрудников правилам безопасности и обучите их, как правильно использовать пароли и другие средства аутентификации.

6. Регулярно обновляйте программное обеспечение и операционные системы, чтобы устранить уязвимости в системе безопасности.

7. Используйте антивирусное программное обеспечение и другие средства защиты от вредоносных программ.

8. Установите брандмауэр и другие средства защиты от внешних атак.

9. Регулярно проводите аудит безопасности, чтобы выявить возможные уязвимости в системе безопасности.

10. Разработайте план действий в случае возникновения инцидента безопасности.

11. Регулярно обновляйте политику безопасности, чтобы она соответствовала текущим требованиям и угрозам.

Следуя этим рекомендациям, вы сможете создать эффективную политику безопасности для своей организации и защитить свои данные и инфраструктуру от кибератак и других угроз.

**Список литературы**

1. Физическая защита: основные принципы и методы обеспечения безопасности // Научные Статьи.Ру — портал для студентов и аспирантов — URL https://nauchniestati.ru/spravka/fizicheskaya-zashhita/
2. Вопросы терминологии и общего подхода к информационной безопасности – URL: <https://tonk.ru/library/article/voprosy-terminologii-i-obshego-podhoda-k-informacionnoj-bezopasnosti#:~:text=%D0%A2%D1%80%D0%B8%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D1%8B%D1%85%20%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B0%2C%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%BC%20%D0%B4%D0%BE%D0%BB%D0%B6%D0%BD%D0%B0,%E2%80%93%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2C%20%D1%86%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2C%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C>
3. Разработка политики информационной безопасности – URL: <https://www.azone-it.ru/razrabotka-politiki-informacionnoy-bezopasnosti>
4. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 01.04.2019) // Собрание законодательства РФ. - 07.01.2002. - № 1 (ч. 1). - Ст. 209.
5. Политика информационно безопасности и хранения персональных данных ПАО Сбербанк – URL: http://www.sberbank.ru/promo/mcqas/documents/user-agreement.pdf