ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.П. Бахар

Учреждение образования «Гродненский государственный университет имени Янки Купалы», Гродно, Беларусь

Техническая защита информации – это комплекс мероприятий и технологий, направленных на обеспечение конфиденциальности, целостности и доступности информации. Она играет ключевую роль в современном информационном обществе, где угрозы безопасности данных постоянно возрастают.

Одним из основных элементов технической защиты информации является шифрование данных. Этот процесс преобразует информацию в нечитаемый формат с помощью специальных алгоритмов, обеспечивая ее защиту от несанкционированного доступа. Современные методы шифрования обеспечивают высокий уровень безопасности и используются в различных сферах, включая банковское дело, здравоохранение и государственные учреждения.

Брандмауэр также является важным компонентом технической защиты информации. Это устройство, которое контролирует поток данных между компьютерными сетями, блокируя нежелательный трафик и защищая сеть от внешних атак. Брандмауэры могут быть реализованы как программное или аппаратное обеспечение и являются неотъемлемой частью современных сетевых систем.

Для обнаружения и удаления вредоносных программ используется антивирусное программное обеспечение. Оно сканирует файлы и системы на наличие вирусов, троянов и других угроз, предотвращая их нанесение ущерба информации. Регулярные обновления баз данных антивирусов обеспечивают эффективную защиту от новых видов вредоносного ПО.

Есть так же средства обнаружения вторжений (Intrusion Detection Systems, IDS) и средства предотвращения вторжений (Intrusion Prevention Systems, IPS) используются для мониторинга и обнаружения несанкционированных попыток доступа или атак на информационные системы. IDS анализируют сетевой трафик и системные журналы

на предмет подозрительной активности, такой как необычные запросы или попытки взлома, и предупреждают администраторов о потенциальных угрозах. IPS, в свою очередь, имеют возможность автоматически реагировать на обнаруженные угрозы, блокируя или изолируя подозрительные устройства или трафик, что позволяет предотвратить возможные атаки до их реализации.

Техническая защита информации требует системного подхода и постоянного обновления мер безопасности в соответствии с изменяющимися угрозами. Эффективное применение технологий шифрования, брандмауэров и антивирусных программ позволяет обеспечить надежную защиту данных и сохранить их целостность и конфиденциальность.

Список литературы

1. Объяснение защиты информации [Электронный ресурс] – Режим доступа: https://www.it-explained.com/words/information-protection-explained-explained – Дата доступа: 03.05.2024.

2. Объяснение защиты информации [Электронный ресурс] – Режим доступа: https://www.prosec-networks.com/en/blog/technischer-datenschutz – Дата доступа: 02.05.2024.