УДК 004.056

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Исмоилов З.Ш., студент 5 курса экономического факультета
Научный руководитель – Лёшина Е.А.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, коммерческая тайна, компьютерные угрозы, информационные технологии, защита информации.*

В работе представлен обзор угроз информационной безопасности на предприятиях. При анализе были установлены основные методы защиты конфиденциальности, целостности, доступности данных для эффективного функционирования предприятия

Информационная безопасность является одной из основных проблем экономической безопасности в современном мире. Распространение применения информационных технологий, стимулирует рост экономики и улучшения работы общественных и государственных институтов, но в то же время зарождает новые информационные угрозы. С ростом возможностей ИТ предприятия осознали важность взаимодействия как конкурентного преимущества.

Наиболее фундаментальной концепцией информационной безопасности является следующие:

- конфиденциальность;
- целостность;
- доступность.

Конфиденциальность – это свойство, которое предотвращает раскрытие информации или ее доступность для неавторизованных процессов, организаций или отдельных лиц.

Целостность данных в информационной безопасности означает обеспечение и поддержание полноты и точности данных на протяжении всего жизненного цикла.

Доступность – это возможность быстро получить необходимую информационную услугу.

Также можно отметить угрозы на предприятиях, связанные с сетевыми инфраструктурами. Основными компонентами сетевой инфраструктуры являются маршрутизаторы, коммутаторы, концентраторы, межсетевые экраны и конечные устройства. Помимо выполнения маршрутизации и других сетевых операций, эти устройства также отвечают за защиту работающих приложений, устройств и серверов от атак и вторжений.

Плохая конфигурация устройства действует как путь для злоумышленника, чтобы использовать данное устройство в своих целях. Распространенными уязвимостями, являются открытый контроль доступа, слабое шифрование и пароли, устройства, использующие настройки установки по умолчанию, и устройства, на которых отсутствуют последние исправления безопасности. Несколько угроз сетевого уровня можно определить как:

- Сниффинг это метод наблюдения и захвата всех пакетов данных, проходящих через сеть;

- Подслушивание, можно определить как несертифицированное сканирование другого целевого сообщения [1].

Информационная безопасность, защита данных, должно состоять в приоритете для эффективного функционирования предприятия.Для этого необходимо осуществлять контроль информационной безопасности, который включает следующие элементы:

- гарантия информации;
- моделирование угроз;
- зонирование сетевой безопасности;
- политика информационной безопасности;
- оценка уязвимости.

Гарантия информации надежна в отношении очень важных компонентов безопасности, таких как целостность, доступность, конфиденциальность и подлинность. После объединения всех этих компонентов информация и информационная система могут быть защищены и гарантированы при использовании, хранении и передаче.

Моделирование угроз – это метод выявления угроз и уязвимостей системы. Прежде чем угроза станет причиной эксплуатации, важно

уделить ей особое внимание и смягчить ее последствия, поскольку они могут повлиять на безопасность приложения.

Это можно сделать, собирая и записывая данные организации и применяя к ним методы идентификации и оценки для анализа информации, которая может повлиять на безопасность. Этот процесс идентификации и проверки выявляет уязвимости среды информационной безопасности.

Зонирование сетевой безопасности можно объяснить как управление и развертывание архитектуры организации в различных зонах безопасности. Эти зоны безопасности могут быть набором сетевых устройств, имеющих определенные уровни безопасности. Зонирование сети с точки зрения их уровней безопасности может быть полезным для контроля и мониторинга потока входящего и исходящего трафика по сети.

Политики информационнойбезопасности — это самый фундаментальный и основной, но зависимый компонент инфраструктуры информационной безопасности [3, 4].

Для защиты данных и ресурсов организации основные требования и правила безопасности настраиваются и применяются в политике информационной безопасности. Эти политики включают административные требования и требования безопасности в отношении информации. Некоторые из важных целей политики информационной безопасности:

- обеспечение информации;
- устранение юридической ответственности;
- защита ресурсов организации;
- предотвращение несанкционированного доступа;
- минимизация риска.

Оценка уязвимости — это метод изучения и анализа возможностей системы или приложений, включая процессы безопасности, запущенные в системе, для борьбы с любой угрозой. С помощью оценки уязвимости можно определить слабые места и угрозы для системы, а также оценить требования и эффективность любого дополнительного уровня безопасности.

Библиографический список:

1. A.L. Buchak and E. Guven Review of Data mining and machine learning methods for detecting cyber security intrusions, IEEE Communication Research Manuals, vol. 18, p. 2, in the second quarter of 2016, pp. 1153-1176

2. Чернышов, Б.В. Определение приоритетных задач в политике (теория научного выбора и опыт истории) / Б.В. Чернышов // Информационная безопасность регионов. - 2014. - № 1. – С.123-128

3. Актуальные киберугрозы: II квартал 2021 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com

4. Гниденко, И.Г. Интеллектуальные системы как вектор развития информационной безопасности предприятия / И. Г. Гниденко, И. В. Егорова, О. Д. Мердина // Петербургский экономический журнал. - 2020. - № 1. – С.147-154

5. Банникова, Е.В. Анализ потенциальных угроз экономической безопасности организации / Е.В. Банникова, О.И. Хамзина, А.А. Навасардян, Е.А. Лёшина // Экономика и предпринимательство. - 2020. - № 11 (124). - С. 816-820.

THE MAIN AREAS OF IMPROVEMENT INFORMATION SECURITY OF THE ENTERPRISE

Ismoilov Z.Sh.

Keywords: *information security, trade secret, computer threats, information technology, information protection.*

The paper presents an overview of threats to information security at enterprises. During the analysis, the main methods of protecting the confidentiality, integrity, and availability of data for the effective functioning of the enterprise were established