**Ф.И.О. преподавателей**: Багрий Е.Н.

**Наименование УД/МДК**: МДК. 06.02 Инженерно-техническая поддержка

**№ урока по КТП**: 09-10 урок

**Тема**: Обеспечение безопасности функционирования информационной системы

**Количество часов**: 2 часа.

**Основная литература**: В.Н. Шитова «Инженерно-техническая поддержка сопровождения информационных систем. (СПО). Учебник.»., В. Д. Алиев, С. Г. Гольдберг, А. С. Ткач "Методы и средства инженерии программного обеспечения". В этой книге рассматриваются различные аспекты применения методов и средств инженерии программного обеспечения, включая вопросы поддержки.

**Цель**: Ознакомление слушателей с основными аспектами обеспечения безопасности функционирования информационной системы. Мы рассмотрим важность обеспечения безопасности, основные принципы и методы обеспечения защиты информационных систем, а также поговорим о контрольных механизмах.

**Основные вопросы, которые мы рассмотрим:**

1. Что такое информационная система и почему обеспечение ее безопасности важно?

2. Какие принципы лежат в основе обеспечения безопасности информационных систем?

3. Какие методы обеспечения безопасности используются в информационных системах?

4. Какие механизмы контроля помогают обеспечивать безопасность функционирования информационных систем?

**Введение:**

Информационная система – это совокупность связанных элементов, таких как компьютеры, сетевое оборудование, программное обеспечение и люди, используемых для сбора, обработки, хранения и передачи информации. Обеспечение безопасности функционирования информационной системы является одним из главных приоритетов для любой организации. Нарушение безопасности информационной системы может привести к серьезным последствиям, включая утечку конфиденциальных данных, нарушение целостности системы и угрозы для бизнес-процессов.

**Основные принципы обеспечения безопасности информационных систем:**

1. Конфиденциальность: принцип, который обеспечивает, что информация доступна только тем лицам, которым она необходима, и защищена от несанкционированного доступа.

2. Целостность: принцип, согласно которому информация в системе должна быть защищена от несанкционированных изменений или повреждений.

3. Доступность: принцип, который гарантирует, что информация доступна только авторизованным пользователям и может быть использована в нужное время.

4. Аутентификация: принцип, согласно которому пользователи должны быть идентифицированы и подтверждены перед тем, как им будет предоставлен доступ к информационной системе.

5. Невозможность отказа: принцип, который предотвращает возможность отрицания совершения определенного действия в информационной системе.

**Методы обеспечения безопасности информационных систем:**

1. Физические меры безопасности: охрана территории, контроль доступа к помещениям с серверами, использование видеонаблюдения и т.д.

2. Криптографические методы: защита информации с помощью шифрования данных, использование цифровых подписей и сертификатов.

3. Сетевая безопасность: обеспечение безопасности данных при передаче по сети с помощью использования брандмауэров, виртуальных частных сетей (VPN) и т.д.

4. Безопасность приложений: устранение уязвимостей в программном обеспечении, проверка безопасности кода, использование защищенных библиотек и фреймворков.

**Механизмы контроля для обеспечения безопасности функционирования информационных систем:**

1. Мониторинг и аудит безопасности: системы и инструменты для отслеживания активности пользователей, обнаружения атак и аномалий.

2. Антивирусные и антишпионские программы: программное обеспечение, предназначенное для обнаружения и уничтожения вредоносных программ.

3. Бэкапы данных: создание резервных копий информации для восстановления после сбоя или атаки.

4. Обучение и осведомленность пользователей: проведение тренингов и обучений для повышения осведомленности пользователей о методах защиты информации и определении атак.

**Контрольные вопросы:**

1. Что такое информационная система и почему обеспечение ее безопасности важно?

2. Назовите 3 принципа обеспечения безопасности информационных систем.

3. Какие методы обеспечения безопасности используются в информационных системах?

4. Какие механизмы контроля помогают обеспечивать безопасность функционирования информационных систем?

**Организация защиты информации, обрабатываемой в информационных системах, основывается на следующих принципах:**

1. Защита ИС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.
2. Защита средств вычислительной техники, входящей в состав ИС, обеспечивается комплексом программно-технических средств.
3. Защита ИС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
4. Защита ИС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики.
6. Неотъемлемой частью работ по защите информации в ИС является оценка эффективности средств защиты.
7. Защита ИС должна предусматривать контроль эффективности средств защиты от НСД.

Ключевая роль в деятельности службы безопасности предприятия должна отводиться аналитико-разведывательному направлению, осуществляющему сбор и обработку информации о конкурентных фирмах и компаниях, о маркетинговых условиях, о криминально-конкурентных действиях. Таким аналитическим звеном может быть отдел обеспечения внешней деятельности подразделения информационно-аналитической работы предприятия.

**Цели и задачи этого подразделения можно сформулировать следующим образом:**

1. выявление фактических возможностей разглашения, утечки и реали­зации способов несанкционированного доступа к конфиденциальным документам, в том числе по косвенным признакам и легальным каналам;
2. прогноз вероятных устремлений конкурентов к конкретным материалам и разработкам предприятия;
3. сбор информации о конкурентах различными способами;
4. выявление причин и обстоятельств, способствующих утечке ком­мерческой информации;
5. оценка надежности и степени защищенности предприятия от внутренних и внешних угроз;
6. участие в анализе, разработке и внедрении комплексных экономически и научно обоснованных мер по защите интересов предприятия.

Одновременно со сбором информации о конкурентах служба безопасности должна пресекать попытки сбора различного рода информации о деятельности своего предприятия. Для этой цели в составе подразделения информационно-аналитической деятельности необходимо организовать котрразведовательный отдел.

Цель контрразведывательного подразделения можно определить как противодействие разведывательным мероприятиям конкурентов и пресечение правонарушений со стороны противоправных групп или отдельных лиц, посягавших на интересы предприятия или его отдельных сотрудников. В отличие от разведки, объектом контрразведывательной деятельности является не внешняя, а внутренняя среда функционирования предприятия. Эта среда включает в себя следующие элементы:

1. Руководящий состав предприятия.

2. Лица из вспомогательного персонала, имеющие доступ к коммерческой тайне.

3. Сотрудники самой службы безопасности.

4. Ранее судимые лица.

5. Сотрудники предприятия, родственники которых работают у конкурентов.

Определение цели и объекта контрразведывательной деятельности позволяет определить круг возможных задач подразделения контрразведки: борьба с экономическим шпионажем, пресечение преступлений против сотрудников, оказание содействия правоохранительным органам в раскрытии преступлений.

**Заключение:**

Обеспечение безопасности функционирования информационной системы является сложным и многогранным процессом, который требует применения различных методов и механизмов защиты. Понимание основных принципов и контрольных механизмов поможет организациям повысить уровень защиты своих информационных систем и минимизировать риски нарушения безопасности.

2. *Оформите в тетради конспект по лекции, сделать отчёт о проделанной работе. Сделать вывод.*

1.Сохранить проект.

2.Сохранить проект. Скриншот вставить в отчет.

3.Сделать вывод о проделанной работе.

4.Оформить занятие в тетрадь и сдать в Google-класс.