ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕДЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 11. ТЕМА 3.2 ОСНОВЫ ИНФОРМАЦИОННОЙ И ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1. Понятие информационной безопасности

Информационная безопасность (ИБ) — состояние защищённости информации, её носителей и инфраструктуры обработки от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб субъектам информационных отношений.

Ключевые свойства защищаемой информации:

- **Конфиденциальность** — доступ к информации имеют только субъекты, обладающие соответствующими правами.
- **Целостность** — информация сохраняется в неизменном виде, исключая несанкционированные модификации.
- **Доступность** — уполномоченные пользователи получают доступ к информации в требуемое время.

В профессиональной деятельности обеспечение ИБ — неотъемлемая часть эксплуатации информационных систем, поскольку нарушение любого из трёх свойств способно привести к финансовым, репутационным и правовым последствиям.

2. Классификация средств защиты информации

Средства защиты информации классифицируются по нескольким основаниям:

По характеру воздействия:

- **Превентивные** — предотвращают возникновение угроз (межсетевые экраны, антивирусные системы, политики паролей).
- **Детективные** — выявляют факты нарушений (системы обнаружения вторжений, журналы аудита, мониторинг событий).
- **Корректирующие** — восстанавливают работоспособность и данные после инцидента (резервное копирование, планы восстановления).

По уровню реализации:

- **Организационные** — политики, регламенты, инструкции, обучение персонала.
- **Технические** — аппаратные и программные решения (шифрование, контроль доступа, межсетевые экраны).
- **Физические** — ограждения, СКУД, видеонаблюдение, сейфы.

По объекту защиты:

- Защита данных (шифрование, разграничение доступа).
- Защита каналов передачи (VPN, TLS).
- Защита узлов и устройств (антивирусы, контроль целостности, доверенная загрузка).

Такая классификация позволяет системно подходить к проектированию защиты в профессиональных информационных системах.

3. Программно-технический уровень защиты

Программно-технический уровень объединяет программные и аппаратные средства, реализующие механизмы защиты на уровне операционных систем, приложений и сетевой инфраструктуры.

Основные компоненты:

- **Средства аутентификации и управления доступом** (Active Directory, LDAP, RBAC) — обеспечивают контроль прав пользователей.

• **Межсетевые экраны (Firewall)** — фильтруют сетевой трафик по правилам и политикам.

• **Системы предотвращения вторжений (IPS)** — анализируют трафик на предмет известных атак и блокируют их.

• **Антивирусные и антималварные решения** — обнаруживают и нейтрализуют вредоносные программы.

• **Средства шифрования** (BitLocker, VeraCrypt, EFS) — защищают данные на дисках и при передаче.

• **Средства контроля целостности** — фиксируют изменения в критически важных файлах и реестрах.

На программно-техническом уровне реализуется большинство механизмов защиты, непосредственно влияющих на повседневную работу пользователей и стабильность информационных систем.

4. Защита жёсткого диска

Жёсткий диск — ключевой носитель данных, требующий комплексной защиты.

Методы защиты:

• **Шифрование диска** (полнодисковое шифрование) — данные хранятся в зашифрованном виде; доступ возможен только при корректной аутентификации. Примеры: BitLocker (Windows), FileVault (macOS), LUKS (Linux).

• **Разделение на логические тома** с разными уровнями доступа — конфиденциальные данные изолируются от общего доступа.

• **Контроль физического доступа** — ограничение доступа к оборудованию, использование замков и сейфов.

• **Резервное копирование** — регулярное создание копий данных на внешних носителях или в облаке.

• **Мониторинг состояния диска** (S.M.A.R.T.) — позволяет прогнозировать отказы и своевременно переносить данные.

Алгоритм действий по защите жёсткого диска:

1. **Оценка критичности данных** — классифицировать информацию по уровню конфиденциальности.
2. **Выбор метода шифрования** — исходя из ОС и требований к производительности.
3. **Настройка шифрования** — активировать полнодисковое шифрование, задать надёжный ключ восстановления.
4. **Разграничение доступа** — настроить права пользователей на уровне файловой системы.
5. **Организация резервного копирования** — запланировать регулярные бэкапы на внешние носители или в облако.
6. **Мониторинг состояния** — настроить сбор и анализ S.M.A.R.T.-данных.
7. **Документирование процедур** — зафиксировать политики и инструкции для администраторов и пользователей.

Такой алгоритм позволяет минимизировать риски потери или утечки данных с жёсткого диска.

5. Защита от компьютерных вирусов и виды компьютерных вирусов

Компьютерный вирус — вредоносная программа, способная к самораспространению, внедрению в другие файлы и выполнению деструктивных действий.

Основные виды компьютерных вирусов:

• **Файловые вирусы** — внедряются в исполняемые файлы (.exe, .dll), активируются при запуске.

• **Загрузочные вирусы** — поражают загрузочные секторы дисков, запускаются до загрузки ОС.

• **Макровирусы** — распространяются через документы с макросами (Word, Excel).

• **Скриптовые вирусы** — используют скрипты (VBScript, JavaScript) для заражения веб-страниц и документов.

• **Сетевые черви** — самостоятельно распространяются по сети, используя уязвимости.

• **Троянские программы** — маскируются под легитимное ПО, выполняют вредоносные действия.

• **Руткиты** — скрывают присутствие вредоносного ПО в системе.

Методы защиты от вирусов:

• **Антивирусное ПО** — регулярно обновляемые базы сигнатур и эвристический анализ.

• **Контроль запуска исполняемых файлов** — использование политик запрета запуска из временных папок и непроверенных источников.

• **Ограничение прав пользователей** — работа под учётной записью с минимальными привилегиями.

• **Регулярное обновление ОС и ПО** — устранение уязвимостей, используемых вирусами.

• **Фильтрация электронной почты и веб-трафика** — блокировка подозрительных вложений и ссылок.

Алгоритм действий при обнаружении вируса:

1. **Изоляция заражённого узла** — отключить компьютер от сети, чтобы предотвратить распространение.
2. **Запуск антивирусного сканирования** — использовать актуальные базы и глубокий режим проверки.
3. **Анализ отчётов сканирования** — определить тип угрозы и затронутые файлы.
4. **Удаление или карантин вредоносных объектов** — по возможности восстановить заражённые файлы.
5. **Проверка целостности системы** — убедиться, что не были изменены критические компоненты ОС.
6. **Смена паролей** — обновить учётные данные, которые могли быть скомпрометированы.
7. **Анализ причин заражения** — выявить источник (вложение, веб-сайт, съёмный носитель) и устранить уязвимость.
8. **Документирование инцидента** — зафиксировать детали для последующего анализа и улучшения защиты.

Этот алгоритм обеспечивает системный подход к реагированию на вирусные инциденты.

6. Организация безопасной работы с компьютерной техникой

Безопасная работа с компьютерной техникой включает как технические, так и организационные меры.

Технические меры:

• Использование лицензионного и обновляемого ПО.

• Настройка автоматического обновления ОС и приложений.

• Включение брандмауэра и антивирусной защиты.

- Ограничение установки стороннего ПО.
- Использование защищённых протоколов передачи данных (HTTPS, SFTP, SSH).

Организационные меры:

- Обучение пользователей основам ИБ (фишинг, пароли, безопасные практики).
- Разработка и внедрение политик ИБ (парольная политика, правила использования съёмных носителей).
- Регулярный аудит прав доступа и журналов событий.
- Документирование инцидентов и анализ причин.

Алгоритм организации безопасной работы:

1. **Разработка политики ИБ** — определить требования к паролям, доступу, использованию устройств.
2. **Настройка технических средств** — активировать антивирус, брандмауэр, шифрование, контроль обновлений.
3. **Обучение персонала** — провести инструктаж по распознаванию фишинга, правилам работы с конфиденциальной информацией.
4. **Внедрение контроля доступа** — назначить права пользователей, ограничить административные привилегии.
5. **Организация резервного копирования** — настроить регулярные бэкапы критически важных данных.
6. **Настройка мониторинга и аудита** — включить журналирование событий, настроить оповещения о подозрительной активности.
7. **Регулярный пересмотр и обновление мер защиты** — анализировать новые угрозы и корректировать политики и настройки.

Соблюдение этого алгоритма позволяет выстроить устойчивую систему защиты в профессиональной среде.