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

ЛЕКЦИЯ 9. ТЕМА 3.3. БЕЗОПАСНОСТЬ, ГИГИЕНА, ЭРГОНОМИКА, РЕСУРСОСБЕРЕЖЕНИЕ. ЗАЩИТА ИНФОРМАЦИИ, АНТИВИРУСНАЯ ЗАЩИТА

Внедрение информационных технологий в профессиональную и повседневную деятельность человека обусловило формирование комплексной проблемы: обеспечение безопасности информационной среды, сохранение здоровья пользователя, рациональное использование вычислительных и энергетических ресурсов, а также экономически обоснованная эксплуатация средств вычислительной техники. Данные аспекты рассматриваются как взаимосвязанные компоненты единой системы организации компьютерного рабочего места, а не как изолированные направления.

1. Защита информации

Защита информации представляет собой деятельность, направленную на обеспечение конфиденциальности, целостности и доступности информации — базовой триады «КЦД» (CIA-триада: Confidentiality, Integrity, Availability). Конфиденциальность предполагает ограничение доступа к данным кругом уполномоченных лиц; целостность — неизменность информации в процессе хранения и передачи; доступность — возможность своевременного получения данных легитимными пользователями.

Нормативную основу защиты информации в Российской Федерации образуют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», а также подзаконные акты и методические документы ФСТЭК России и ФСБ России. Обработка персональных данных допускается исключительно при наличии законного основания (согласие субъекта, исполнение договора, требования законодательства), при этом объём обрабатываемых данных должен соответствовать заявленным целям обработки, а хранение — ограничиваться сроком достижения этих целей. Законодательство последовательно ужесточается: операторы обязаны регистрироваться в реестре Роскомнадзора, обеспечивать локализацию баз данных граждан РФ на территории России, а за утечку персональных данных предусматриваются штрафы, достигающие нескольких миллионов рублей.

Классификация угроз защиты информации включает:

- **несанкционированный доступ** — получение информации лицом, не имеющим права на её чтение или изменение;
- **вредоносное программное обеспечение** (вирусы, трояны, шпионские программы, программ-вымогателей);
- **атаки на уязвимости программного обеспечения** — межсайтовый скриптинг (XSS), SQL-инъекции, инъекции команд; по данным MITRE и CISA, именно эти классы ошибок входят в число наиболее распространённых и опасных проблем современного программного обеспечения, ставших причиной десятков тысяч зарегистрированных уязвимостей;
- **социальную инженерию** — манипулирование пользователем с целью получения конфиденциальных сведений (фишинг, вивисекция);
- **утрату данных вследствие аппаратных сбоев** и человеческого фактора.

Основные методы защиты сводятся к организационным (регламентация доступа, обучение персонала, резервное копирование) и техническим (идентификация и аутентификация, разграничение прав доступа, шифрование, межсетевое экранирование, средства обнаружения вторжений). Резервное копирование по принципу «3-2-1» — три копии данных на двух типах носителей, одна из которых хранится вне основной площадки, — остаётся базовой практикой обеспечения устойчивости к утрате данных.

2. Антивирусная защита

Антивирусная защита является подсистемой комплексной безопасности, ориентированной на выявление, блокирование и удаление вредоносного программного обеспечения. Актуальность задачи подтверждается статистикой: количество публикуемых уязвимостей ежегодно растёт; так, в третьем квартале 2025 года число зарегистрированных CVE более чем на тысячу превысило показатель аналогичного периода 2024 года, при этом злоумышленники продолжают активно эксплуатировать давно закрытые, но не устранённые на машинах пользователей уязвимости в Microsoft Office и архиваторах.

Современные антивирусные средства реализуют многоуровневый подход:

1. **сигнатурный анализ** — сопоставление кода файлов с базой известных вредоносных образцов; эффективен против известных угроз, но беспомощен перед новыми;
2. **эвристический анализ** — выявление подозрительных структур кода и поведения, позволяющий обнаруживать модификации известных угроз;
3. **поведенческий анализ (HIPS)** — мониторинг действий программ в реальном времени и блокирование типичного для вредоносного ПО поведения (массовое шифрование файлов, модификация системных ключей реестра);
4. **облачные технологии** — мгновенная проверка репутации файлов на серверах разработчика;
5. **защитные функции смежного характера** — фаервол, контроль запуска приложений, защита от фишинга и шифровальщиков.

Ключевым условием эффективности антивирусной защиты является регулярное обновление сигнатурных баз, поскольку их актуальность определяет способность системы распознавать новые образцы вредоносного ПО. Вместе с тем сами средства защиты являются частью программной среды и также подвержены уязвимостям, что подтверждается регистрацией соответствующих записей в банке данных уязвимостей ФСТЭК России; это обусловливает необходимость своевременной установки обновлений и продуктовых патчей.

Организационные меры антивирусной защиты включают: запрет или ограничение запуска исполняемых файлов из недоверенных источников, проверку съёмных носителей, использование учётных записей с минимально необходимыми привилегиями, регулярное обновление операционной системы и прикладного ПО, а также резервное копирование критически важных данных на изолированные носители.

3. Эксплуатационные требования к компьютерному рабочему месту

Компьютерное рабочее место как элемент производственной среды регламентируется санитарными нормами и правилами охраны труда. В настоящее время действуют СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания», СП 2.2.3670-20 «Санитарно-эпидемиологические требования к условиям труда» и приказ Минтруда России от 29.10.2021 № 774н, установивший единые требования к организации рабочих мест. Ранее действовавший СанПиН 2.2.2/2.4.1340-03, посвящённый работе с ЭВМ, с 1 января 2021 года отменён.

Гигиенические требования к организации рабочего места включают следующие группы параметров:

- **площадь рабочего места** — на одно рабочее место с персональным компьютером должно отводиться не менее 4,5 м²;
- **визуальные эргономические параметры монитора** — расстояние от глаз пользователя до экрана (рекомендуется 50–70 см), расположение экрана ниже уровня глаз, регулировка яркости и контрастности;
- **освещённость** — сочетание естественного и искусственного освещения; исключение бликов на экране;

• **микроклимат, уровни шума, вибрации, электромагнитных полей** — регламентируются предельно допустимыми значениями в соответствии с СанПиН 1.2.3685-21.

Особое значение имеет нормирование продолжительности работы с электронными средствами обучения и информации. Для учащихся установлены предельные значения непрерывного использования персонального компьютера на уроке: 20 минут для 1–2 классов, 25 минут для 3–4 классов, 30 минут для 5–9 классов, 35 минут для 10–11 классов.

Эргономические требования предусматривают рациональную организацию рабочей позы: исключение длительных статических нагрузок с наклоном и поворотом туловища, свободное положение ног, оптимальную высоту рабочей поверхности и сидения. Профилактические меры включают перерывы в работе, гимнастику для глаз и опорно-двигательного аппарата, а также регулярную дезинфекцию поверхностей устройств.

4. Ресурсосбережение при эксплуатации вычислительной техники

Ресурсосбережение в контексте информационных технологий охватывает экономию электроэнергии, рациональное использование аппаратных ресурсов и продление срока службы оборудования. Типичный настольный компьютер средней мощности потребляет порядка 200–250 Вт, из которых на системный блок приходится 150–200 Вт, на монитор — около 50 Вт; в режиме ожидания потребление снижается до 85–105 Вт, а в спящем режиме — в десять и более раз по сравнению с активной работой.

Основные направления экономии энергии:

• перевод компьютера в спящий режим или его отключение при перерывах в работе и по окончании рабочего дня;

• настройка планов электропитания операционной системы (автоматическое отключение дисплея, снижение производительности в режиме простоя);

• рациональная настройка яркости и контрастности монитора;

• отключение периферийных устройств, не используемых в текущий момент.

Аппаратный аспект ресурсосбережения связан с управлением жизненным циклом техники: своевременная профилактика (очистка систем охлаждения, контроль температурного режима) снижает износ компонентов; модернизация отдельных элементов (увеличение объёма оперативной памяти, замена накопителя на твердотельный) позволяет продлить срок эксплуатации изделия без полной замены. Отдельного внимания требует утилизация отработавших изделий: электронные изделия содержат ценные и токсичные материалы и подлежат переработке в рамках специально организованных пунктов приёма.

5. Экономические аспекты применения информационных технологий

Экономическая оценка информационных технологий опирается на понятие совокупной стоимости владения (Total Cost of Ownership, TCO), введённое в аналитическую практику компанией Gartner. TCO представляет собой сумму всех расходов на актив за весь период его использования: первоначальные инвестиции (оборудование, лицензии, внедрение), операционные расходы (техническая поддержка, обновления, электроэнергия, персонал, обучение), а также скрытые издержки — простои систем, снижение производительности, риски нарушения требований регуляторов. Существенно, что косвенные затраты могут составлять 60–70 % совокупной стоимости владения, вследствие чего оценка лишь стартовой цены решения приводит к систематически искажённым выводам при выборе между альтернативами (собственная инфраструктура или облачная аренда, бессрочная лицензия или подписка).

Экономический эффект применения информационных технологий формируется за счёт: повышения производительности труда, сокращения времени выполнения операций, снижения числа ошибок, ускорения документооборота и принятия решений. При этом затраты на обеспечение информационной безопасности целесообразно рассматривать не

как издержки, а как инвестиции в снижение вероятного ущерба: стоимость инцидента (восстановление данных, простои, штрафы, репутационные потери) многократно превышает расходы на превентивные меры — лицензионное антивирусное ПО, резервирование, обучение персонала.

Энергетическая составляющая также поддаётся количественной оценке: при тарифе около 4–7 рублей за киловатт-час непрерывная работа компьютера обходится в тысячи рублей в год, что делает энергосберегающие режимы экономически значимым фактором эксплуатации.

Комплексная организация компьютерного рабочего места предполагает согласованное решение трёх взаимосвязанных задач: защита информации обеспечивается сочетанием правовых, организационных и программно-технических мер при центральном значении антивирусной защиты и регулярного обновления программной среды; сохранение здоровья пользователя достигается соблюдением гигиенических и эргономических нормативов, установленных действующими санитарными правилами; рациональное ресурсопользование и управление совокупной стоимостью владения формируют экономически устойчивую модель эксплуатации информационных технологий на всём жизненном цикле технических и программных средств.