Лекция №1

Информационная безопасность: основные понятия и определения

Вопросы темы:

1. Цели и задачи предмета «Безопасность и управление доступом в ИС»
2. Понятие информационной безопасности.
3. Основные составляющие информационной безопасности.
4. Важность и сложность проблемы информационной безопасности.

1.Цели и задачи предмета «Безопасность и управление доступом в ИС»

Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков.

Актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается.

Проблема защиты информации является многоплановой и комплексной. Современное развитие электроники, технических средств обработки, хранения и защиты информации происходит интенсивно. Одновременно совершенствуются и средства несанкционированного доступа и использования как на программном, так и на программно-аппаратном уровне.

Необходимо знать :

1. источники возникновения информационных угроз;
2. Модели и принципы защиты информации от несанкционированного доступа;
3. Методы антивирусной защиты информации;
4. Состав и методы организационно-правовой защиты информации;
5. Принципы организации разноуровнего доступа в АИС

Необходимо уметь:

1. Применять правовые, организационные, технические и программные средства защиты информации;
2. Назначать доступ к файловым ресурсам и обеспечивать их безопасность.

Основные разделы дисциплины:

Раздел I. Основы безопасности в АИС.

Раздел II. Организационно-правовое обеспечение безопасности в АИС.

Раздел III. Основные принципы построения систем защиты информации.

Раздел IV. Управление доступом в информационных системах.

Раздел V. Вирусы и антивирусная защита.

Раздел VI. Основные программно-технические меры.

2. Понятие информационной безопасности.

Под информацией (информационным обеспечением) понимается любой вид накапливаемых, хранимых и обрабатываемых данных.

Движение информации в ЭВМ неразрывно связано с функционированием программ ее обработки и обслуживания (информационное программное обеспечение).

Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления **субъектов информационных отношений** и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от **поддерживающей инфраструктуры**, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

3. Основные составляющие информационной безопасности.

Информационная безопасность - многогранная, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

- **Доступность** - это возможность за приемлемое время получить требуемую информационную услугу.
- Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- **Конфиденциальность** - это защита от несанкционированного доступа к информации.

Основные принципы обеспечения информационной безопасности предприятия

1. Обеспечение целостности и сохранности данных;
2. Соблюдение конфиденциальности информации;
3. Доступность информации для всех авторизованных пользователей при условии контроля за всеми процессами использования ими получаемой информации
4. Беспрепятственный доступ к информации в любой момент, когда она может понадобиться предприятию.

Для реализации данных принципов необходима интегрированная система информационной безопасности, выполняющая следующие функции:

- Выработку политики информационной безопасности;
- Анализ рисков (ситуаций, в которых может быть нарушена нормальная работа ИС, а также утрачены или рассекречены данные);
- Планирование мер по обеспечению ИБ;
- Планирование действий в чрезвычайных ситуациях;
- Выбор технических средств обеспечения ИБ.

Политика ИБ определяет:

- Какую информацию и от кого (чего) следует защищать;
- Кому и какая информация требуется для выполнения служебных обязанностей;
- Какая степень защиты необходима для каждого вида информации;
- Чем грозит потеря того или иного вида информации;
- Как организовать работу по защите информации.

4. Важность и сложность проблемы информационной безопасности.

Защита информации (ЗИ) – комплекс мероприятий, направленных на обеспечение важнейших аспектов ИБ: доступности, целостности и конфиденциальности.

Система называется безопасной (надежной), если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Система считается надежной, если она, с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются: политика безопасности и гарантированность.

Политика безопасности отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организации при обработке, защите и распространении информации.

Гарантированность показывает насколько корректно выбраны механизмы, обеспечивающие безопасность системы.

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности системы (должен использоваться механизм подотчетности, протоколирования, дополняющийся анализом заполненной информации, т.е. аудитом).

Формирование режима ИБ – проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

1. Законодательный (законы, нормативные акты, стандарты и т.д.)
2. Административный (действия общего характера, предпринимаемые руководством организации)
3. Процедурный (конкретные меры безопасности, имеющие дело с людьми)
4. Программно-технический (конкретные технические меры).

Контрольные вопросы:

1. Каковы цели и задачи изучения дисциплины «Безопасность и УД»?
2. Что понимают под ИБ?
3. Что такое защита информации (ЗИ)?
4. Назовите основные составляющие ИБ.
5. В каком случае можно считать систему надежной (защищенной)?
6. Каковы критерии оценки надежности системы?
7. Назовите основные уровни ИБ.

Дополнительные задания:

- Подобрать материал к докладу «Основные составляющие безопасности АИС»
- Подобрать материал к реферату

1. «Виды угроз в АИС»
2. «Программно-аппаратные методы защиты»