Лекция 1. Введение и основные понятия

1. Современное состояние информационных технологий. Проблема защиты информации и подходы к ее возможному решению.
2. Основные понятия информационной безопасности.
3. Угрозы безопасности информации.

Литература

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах.
2. Хорев П.Б. Программно-аппаратная защита информации.
3. Хорев П.Б. Защита информационных систем.

Дополнительная литература

1. Хорев П.Б. Криптографические интерфейсы и их использование.
2. Хорев П.Б. Лабораторный практикум по методам и средствам защиты информации.
3. Галатенко В.А. Стандарты информационной безопасности.
4. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах.

Проблема защиты информации

Надежное обеспечения сохранности информации и установленного статуса ее использования.

Особенности современных информационных технологий

- увеличение количества автоматизированных процедур в системах обработки данных и важности принимаемых на их основе решений;
- территориальная распределенность компонентов компьютерных систем и передача информации между этими компонентами;
- усложнение используемых программных и аппаратных средств компьютерных систем;

Особенности современных информационных технологий

- накопление и долговременное хранение больших массивов данных на электронных носителях, зачастую не имеющих твердых копий;
- интеграция в единых базах данных информации различного назначения и различных режимов доступа;

Особенности современных информационных технологий

- непосредственный доступ к ресурсам компьютерных систем большого количества пользователей различных категорий и с различными полномочиями в системе;
- рост стоимости ресурсов компьютерных систем.

Подходы к защите компьютерной информации

1. Фрагментарный подход - применяются отдельные организационные мероприятия, технические и программные средства (антивирусные программы, не всегда своевременно обновляемые, и средства разграничения прав пользователей компьютерной системы на основе паролей, часто простых и редко обновляемых).

Подходы к защите компьютерной информации

2. Системный – создается целостная система со своим управляющим блоком (ядром защиты), которая должна обеспечивать надежную защиту компьютерной системы во все время ее функционирования.

Подходы к защите компьютерной информации

3. Комплексный – защита компьютерной информации рассматривается не как одноразовая акция, а как непрерывный процесс, целенаправленно проводимый во все время создания и функционирования компьютерной системы с комплексным применением всех имеющихся методов, средств и мероприятий.

Основные понятия защиты информации

- Под *информацией*, применительно к задаче ее защиты, понимают сведения (сообщения, данные) независимо от формы их представления. В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную.

Формы представления информации

- К *документированной* информации (или просто к *документам*) относят информацию, представленную на материальных носителях вместе с идентифицирующими ее реквизитами. *Речевая* информация возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения. *Телекоммуникационная* информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче.

Информационные процессы, технологии и системы

- К *информационным процессам* относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации. Под *информационной системой* понимают упорядоченную совокупность *информационных ресурсов (*документов и массивов документов) и *информационных технологий* (методов и программно-аппаратных средств), реализующих информационные процессы.

Компьютерная система

- Под компьютерной системой понимают организационно-техническую систему, включающую в себя информационные ресурсы, программно-аппаратные средства, а также обслуживающий персонал и пользователей.

Виды информации

- Информацию разделяют на *общедоступную* и *ограниченного доступа*. К информации ограниченного доступа относятся государственная тайна и конфиденциальная информация. В соответствии с российским законодательством к конфиденциальной относится следующая информация:
- служебная тайна (например, тайна суда и следствия);
- профессиональная тайна (врачебная, адвокатская и т.п.);
- коммерческая тайна;
- персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).

Обладатель информации

Обладателем информации может быть физическое или юридическое лицо, Российская Федерация, ее субъект, муниципальное образование, которое:

- самостоятельно создало информацию

или

- в соответствии с законодательством или договором получило право управлять доступом к информации.

Защищаемая информация

- К *защищаемой* относится информация, имеющая обладателя и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации. *Зашитой информации* называют деятельность по предотвращению
- утечки защищаемой информации,
- несанкционированных и
- непреднамеренных воздействий на защищаемую информацию.

Характеристики защищенности информации

- *Конфиденциальность (*известность содержания информации только имеющим соответствующие полномочия субъектам). Конфиденциальность является субъективной характеристикой информации, связанной с объективной необходимостью защиты законных интересов одних субъектов от других.

Характеристики защищенности информации

- *Целостность* (неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения). Целостность является частью более широкой характеристики информации – ее достоверности, включающей помимо целостности еще полноту и точность отображения предметной области.

Характеристики защищенности информации

- *Доступность* (способность обеспечения беспрепятственного доступа субъектов к интересующей их информации). *Отказом в обслуживании* называют состояние информационной системы, при котором блокируется доступ к некоторому ее ресурсу.

Утечка (копирование) информации

- Под *утечкой* понимают неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получениями разведками. *Разглашение* – это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати). *Несанкционированный доступ* – получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

Воздействие на информацию (модификация, подмена, уничтожение)

- *Несанкционированное воздействие* на защищаемую информацию – воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода или умышленная подмена электронного документа).

Воздействие на информацию

- Под *непреднамеренным воздействием* на защищаемую информацию понимают воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).

Цель и объекты защиты

- *Целью* защиты информации (ее желаемым результатом) является предотвращение ущерба обладателю или пользователю информации. Под *эффективностью* защиты информации понимают степень соответствия результатов защиты информации поставленной цели. *Объектом защиты* может быть информация, ее носитель или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью.

Информационная безопасность и политика безопасности

- Совокупность информационных ресурсов и системы формирования, распространения и использования информации называют *информационной средой* общества. Под *информационной безопасностью* понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие. *Политика безопасности* – это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Угрозы безопасности

- Под *угрозой* безопасности информации в компьютерной системе (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. *Уязвимость информации* – это возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атака на компьютерную систему

- *Атакой* на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является попыткой реализации угрозы безопасности информации в ней.

Цели угроз безопасности информации

- Нарушение конфиденциальности (перехват, утечка или копирование информации).
- Нарушение целостности (разрушение, модификация или подделка информации).
- Нарушение доступности (блокирование информации или отказ в обслуживании).

Угроза раскрытия параметров

- Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.

Естественные и искусственные угрозы

- Угрозы информационной безопасности могут быть разделены на угрозы, не зависящие от деятельности человека (*естественные* угрозы физических воздействий на информацию стихийных природных явлений), и угрозы, вызванные человеческой деятельностью (*искусственные* угрозы, которые являются гораздо более опасными).

Искусственные угрозы

- Искусственные угрозы, исходя из их мотивов, разделяются на *непреднамеренные* (случайные) угрозы и угрозы *преднамеренные* (умышленные). К непреднамеренным угрозам относятся:
- ошибки в проектировании КС;
- ошибки в разработке программных средств КС;
- случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
- ошибки пользователей КС;
- воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

Умышленные угрозы

К умышленным угрозам относятся:

- несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
- несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

Построение модели угроз

- Поскольку сложно заранее определить возможную совокупность угроз безопасности информации и результатов их реализации, модель потенциальных угроз безопасности информации в КС должна создаваться совместно собственником (владельцем) КС и специалистами по защите информации на этапе проектирования КС. Созданная модель должна затем уточняться в ходе эксплуатации КС.