
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Проблемы и перспективы развития ИТ

Лекция 1

**Основные требования к
информационной безопасности**

План лекции

- **Основные понятия информационной безопасности**
- **Угрозы и уязвимость**
- **Модель нарушителя**

1. Информационная безопасность.

Основные понятия

Информационная безопасность (ИБ) - **состояние защищенности национальных интересов в информационной сфере**, определяемых совокупностью сбалансированных интересов личности, общества и государства.

❖ **Закон РК «Об участии в международном информационном обмене»:**

ИБ - **состояние защищенности информационной среды общества**, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

1. Информационная безопасность.

Основные понятия

Обеспечение информационной безопасности предполагает сохранение (поддержание) на требуемом уровне **трех характеристик информации:**

- **конфиденциальности;**
- **целостности;**
- **доступности.**

Конфиденциальность информации состоит в запрете на ознакомление с нею кого бы то ни было за исключением лиц (физических или юридических), имеющих на это право.

1. Информационная безопасность.

Основные понятия

Целостность информации – характеризует отсутствие искажений (порчи) элементов данных, а также отсутствие нарушения логических связей и несогласованности между ними.

Доступность информации – это возможность за приемлемое время получить требуемую информационную услугу.

1. Информационная безопасность.

Основные понятия

Конкретная трактовка термина "**информационная безопасность**" в значительной степени зависит от того, **какая из** названных **характеристик информации** (или их сочетание) **подвергается угрозе**, и **какая технология** может быть **использована для предотвращения этой угрозы**.

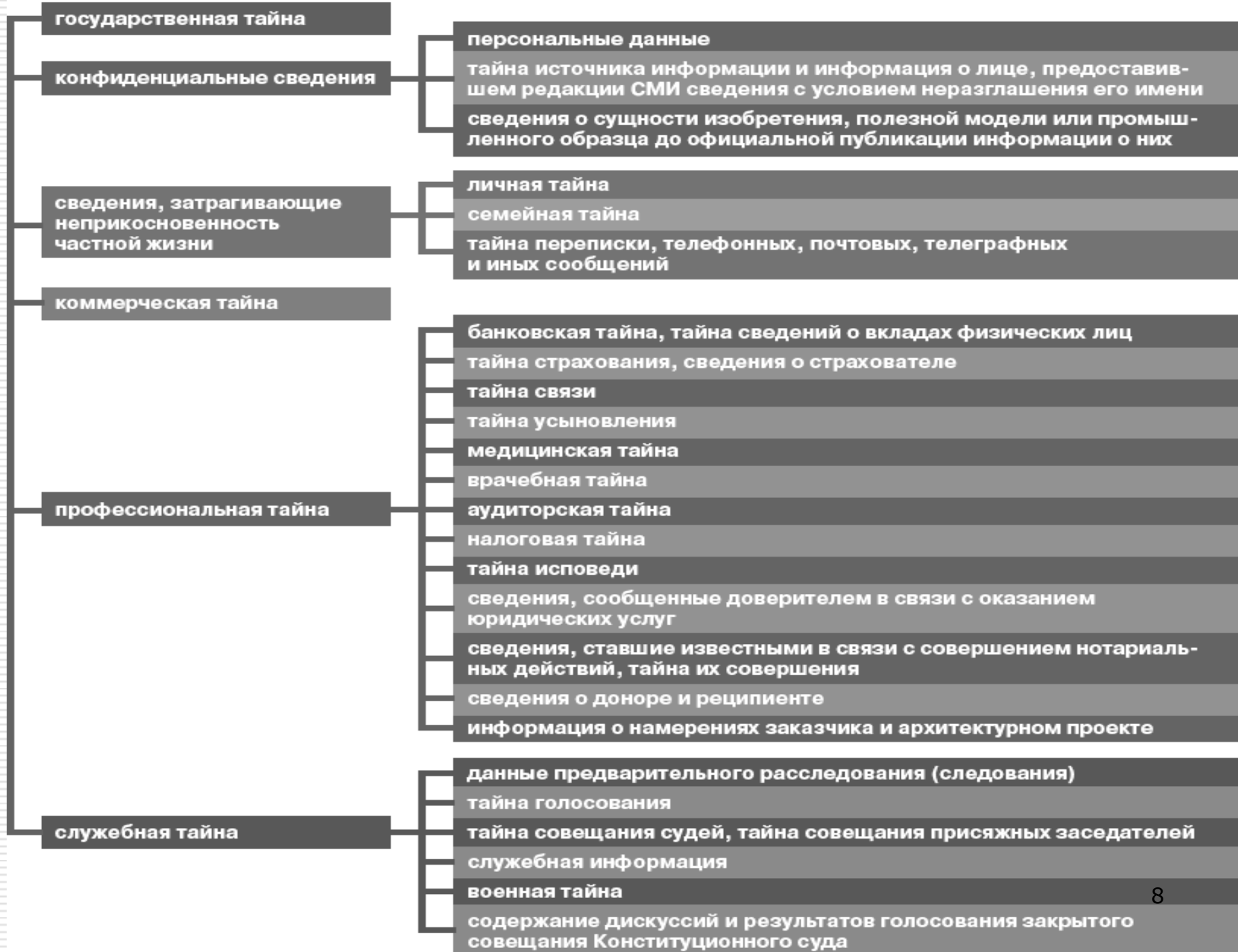
Комплекс мероприятий, направленных на обеспечение информационной безопасности, называется **защитой информации**.

1. Информационная безопасность.

Основные понятия.

Виды конфиденциальной **информации**
с ограниченным доступом:

- 1. Государственная тайна;**
- 2. Конфиденциальные сведения;**
- 3. Сведения, затрагивающие неприкосновенность частной жизни;**
- 4. Коммерческая тайна;**
- 5. Профессиональная тайна;**
- 6. Служебная тайна**



1. Информационная безопасность.

Основные понятия

Организационные методы защиты конфиденциальной информации

Организационные меры обеспечения безопасности ориентированы на людей, а не на технические средства.

Люди формируют и реализуют режим информационной безопасности, и они же оказываются главной угрозой для этой безопасности. Именно поэтому "человеческий фактор" заслуживает особого внимания.

1. Информационная безопасность.

Основные понятия

Классы организационных мер:

- 1. управление персоналом;**
- 2. организация физической защиты;**
- 3. поддержание исходного уровня защищенности системы;**
- 4. реагирование на нарушения режима безопасности;**
- 5. разработка политики безопасности.**

Организационные методы защиты конфиденциальной информации

Управление персоналом

Разделение обязанностей

Минимизация привилегий

Подбор персонала

Обучение

Беседа с увольняемыми

Организация физической защиты

Управление физическим доступом

Противопожарная защита

Защита инфраструктуры

Защита мобильных систем

Поддержание защищенности

Поддержка пользователей

Сопровождение ПО

Организация резервного копирования

Документирование

Организация регламентных работ

Реагирование на нарушения безопасности

Локализация инцидента

Выявление нарушителя

Предупреждение повторных нарушений

Разработка политики безопасности

Политика верхнего уровня

Политика среднего уровня

Политика нижнего уровня
(системная политика)

1. Информационная безопасность.

Основные понятия

Организация физической защиты

К **мерам** физической защиты относятся:

1. управление физическим доступом к средствам обработки, хранения и передачи информации;
2. меры противопожарной защиты;
3. защита поддерживающей инфраструктуры;
4. защита мобильных систем.

1. Информационная безопасность.

Основные понятия

Меры управления физическим доступом

направлены на ограничение числа и контроль за действиями лиц, имеющих возможность влиять на безопасность информации.

Контролироваться может все здание организации, а также отдельные технологические и административные помещения. Например, такие, в которых установлены серверы, коммуникационная аппаратура, хранятся резервные копии данных и программ и т.п.

1. Информационная безопасность.

Основные понятия

К **поддерживающей инфраструктуре** можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций.

В принципе, к ним применимы те же требования, что и к самим информационным системам. Оборудование нужно защищать от краж и повреждений, использовать варианты моделей с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

1. Информационная безопасность.

Основные понятия

Под защитой мобильных систем

понимается **предотвращение инцидентов** с переносными и портативными компьютерами (ноутбуками, карманными ПК и т.д.).

Наиболее распространенными инциденты - их кражи и утери. Соответственно, организационные меры должны быть направлены, с одной стороны, на снижение вероятности таких происшествий, а с другой – **на затруднение доступа к данным, хранящимся в «утраченном» мобильном компьютере.**

Специальные средства: пароли, шифрование, самоликвидация в случае несанкционированного доступа к данным.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Виды угроз безопасности

Под **угрозой безопасности** информационной системы мы будем понимать **потенциально возможное событие**, которое в случае его реализации способно оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Возможные угрозы подразделяются **на три вида**:

- 1. Нарушение конфиденциальности** – данные становятся известны тому, кто их знать не должен;

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

2. Нарушение целостности – данные частично или полностью изменяются (модифицируются) вопреки желанию их владельца;

например, нарушением целостности является изменение стиля форматирования документа или изменение логических связей между элементами базы данных;

3. Нарушение доступности – некоторые (или даже все) сервисы, реализуемые информационной системой, и/или предоставляемые ими данные становятся недоступны пользователям;

примеры таких ситуаций: невозможность считывания файлов с FTP-сервера из-за его перегруженности; отказ пользователю в подключении к системе вследствие умышленной подмены его пароля.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Угрозы могут быть связаны как со случайными факторами, так и с преднамеренными действиями злоумышленников.

Угрозы первого рода называют

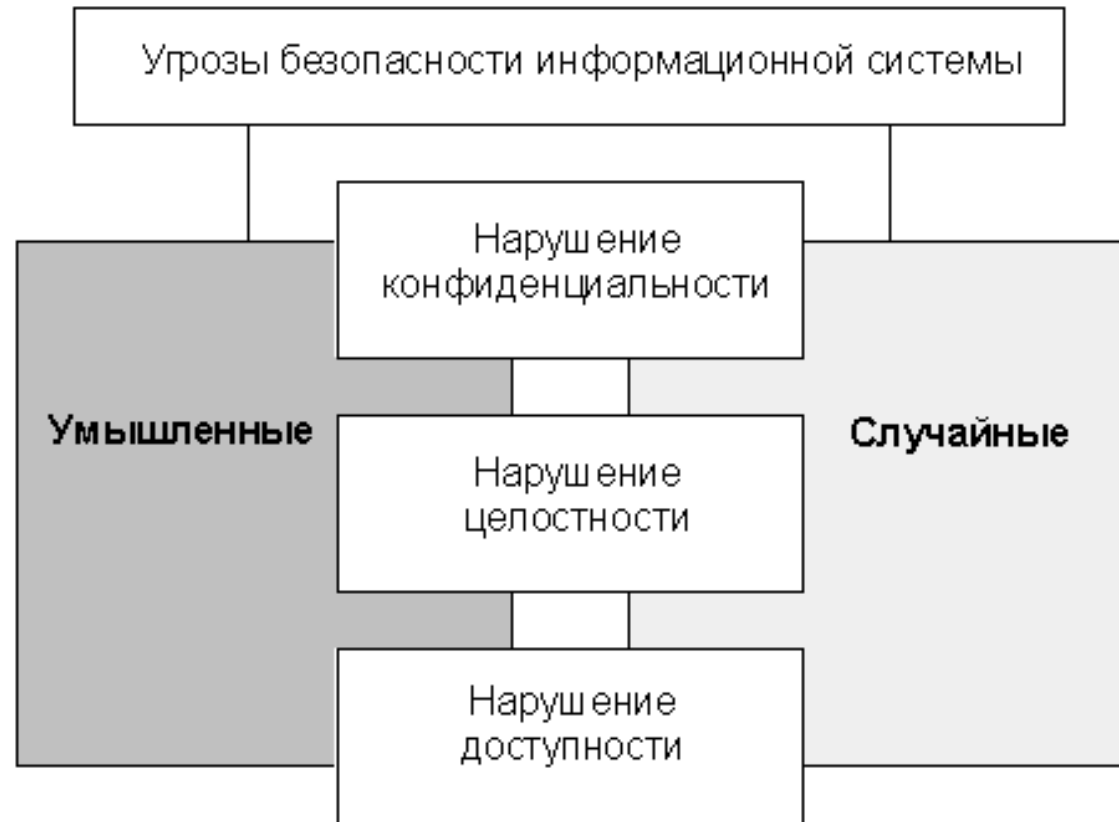
случайными

(непреднамеренными)

а угрозы второго рода –

умышленными

(преднамеренными)



1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Угроза – это **потенциально возможное событие**, то есть такое, вероятность которого для данной информационной системы больше нуля.

Список угроз безопасности конкретной информационной системы определяется перечнем ее **уязвимостей**.

Уязвимость – это **свойство информационной системы**, которое делает возможной реализацию угрозы.

Например, подключение компьютера к сети Интернет делает его уязвимым для сетевых вирусов;

отсутствие средств контроля за состоянием жесткого диска компьютера делает возможным потерю (нарушение целостности) записанных на нем данных.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Степень уязвимости и уровень соответствующей ей угрозы есть величины, связанные прямой зависимостью: **чем выше степень уязвимости, тем выше вероятность соответствующей ей угрозы.**

Применительно к умышленным угрозам используется еще одно важное понятие – **атака**.

Атака – это **поиск и/или использование злоумышленником уязвимости** системы.

Другими словами, **атака – это действия, направленные на реализацию угрозы.**

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Случайные угрозы

«Все, что может случиться, – случается, что не может случиться, – случается тоже» – гласит известный закон Мэрфи.

наиболее вероятные **угрозы случайного характера**:

- **ошибки обслуживающего персонала и пользователей**;
- **потеря информации**, обусловленная неправильным хранением данных;
- **сбои и отказы** аппаратной части компьютера;
- **перебои электропитания**;
- **стихийные бедствия и аварии** технологических систем;
- **некорректная работа** программного обеспечения;
- **непреднамеренное заражение системы компьютерными вирусами** или другими видами вредоносного программного обеспечения.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Умышленные угрозы

Умышленных угроз следует опасаться тому, кто считает, что у него есть враги (недоброжелатели), недобросовестные конкуренты или, по крайней мере, друзья, способные на соответствующие «шутки».

Наиболее серьезную опасность представляют следующие **виды умышленных угроз**:

- **внедрение в систему вирусов** или иного вредоносного программного обеспечения;
- **кража носителей данных** и печатных документов;
- **умышленное разрушение** информации или полное ее уничтожение;
- **злоупотребление полномочиями**;
- **перехват** электромагнитных излучений.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Виды угроз при работе в сети:

- **несанкционированный доступ** к сетевым ресурсам;

например, злоумышленник может воспользоваться принтером, подключенным к компьютеру, работающему в сети (он вряд ли захочет затем забрать распечатку, но объем выводимых данных может привести к исчерпанию картриджа или блокированию принтера);

- **раскрытие и модификация данных** и программ, их копирование;

например, злоумышленник может, получив доступ к жесткому диску компьютера, отыскать на нем сетевое имя и пароль пользователя, под которым тот подключается к Интернету;

- **несанкционированное копирование** данных и программ;

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

- **раскрытие, модификация или подмена** трафика вычислительной сети;
характерный пример – «бомбардировка» почтового сервера фиктивными письмами, что способно привести к перегрузке сервера;
- **фальсификация сообщений**, отказ от факта получения информации или изменение времени ее приема;
например, недобросовестный клерк банка может фальсифицировать заявку на перечисление некоторой суммы со счета клиента;
- **перехват и ознакомление с информацией**, передаваемой по каналам связи;
скажем, если вы решите заказать через Интернет железнодорожные билеты с доставкой на дом, то злодеи вполне могут узнать и адрес, и период времени, в течение которого хозяева будут в отъезде.

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Несанкционированный доступ к информации

НСД – это доступ к информации, нарушающий установленные правила разграничений и осуществляемый с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС).

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

Под **штатными средствами** СВТ и АС понимается совокупность их программного, микропрограммного и технического обеспечения.

Характерными **примерами НСД** являются:

- вход пользователя в систему под чужим паролем;
 - обращение программы к той области памяти (данным), к которой она, в соответствии с ее декларированными функциями, обращаться не должна.
-

1. Информационная безопасность.

Основные понятия. Угрозы и уязвимости

К основным **способам НСД** относятся:

- **непосредственное обращение** к объектам доступа;
- **создание программных и технических средств**, выполняющих обращение к объектам доступа в обход средств защиты;
- **модификация средств защиты**, позволяющая осуществить НСД;
- **внедрение** в технические средства СВТ или АС **программных или технических механизмов**, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

1. Информационная безопасность.

Основные понятия. Модель нарушителя

Модель нарушителя – это абстрактное (обобщенное) описание лица, осуществляющего НСД.

В качестве нарушителя рассматривается **субъект, имеющий доступ к работе со штатными средствами АС и СВТ** как части АС.

Нарушители **классифицируются по:**

А. Уровню возможностей,
предоставляемым им штатными средствами АС и СВТ.

1. Информационная безопасность.

Основные понятия. Модель нарушителя

Различают **4 уровня возможностей** (каждый последующий содержит предыдущий):

1 уровень - самый низкий; предполагает **возможность запуска задач (программ) из фиксированного набора**, реализующих заранее предусмотренные функции по обработке информации;

2 уровень - **возможность создания и запуска собственных программ** с новыми функциями по обработке информации;

1. Информационная безопасность.

Основные понятия. Модель нарушителя

3 уровень - возможность управления функционированием АС, т.е. воздействия на базовое программное обеспечение и на состав и конфигурацию ее оборудования;

4 уровень - весь объем возможностей по проектированию, реализации и ремонту технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

1. Информационная безопасность.

Основные понятия. Модель нарушителя

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

1. Информационная безопасность.

Основные понятия. Модель нарушителя

нарушителей можно **классифицировать** (продолжение):

Б. По уровню действий (используемым методам и средствам):

- **применяющий методы получения сведений** от людей (в т.ч. и социальная инженерия);
- **применяющий пассивные средства** (технические средства перехвата без модификации компонентов системы);
- **использующий только штатные средства и недостатки систем защиты** для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные носители информации, которые могут быть скрытно пронесены через посты охраны;

1. Информационная безопасность.

Основные понятия. Модель нарушителя

- **применяющий методы и средства активного воздействия** (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

В. По времени действия:

- **в процессе функционирования ИС;**
- **в период пассивности компонентов системы** (нерабочее время, плановые перерывы в работе, перерывы для обслуживания и ремонта и т.п.);
- **как в процессе функционирования ИС, так и в период пассивности** компонентов системы.

1. Информационная безопасность.

Основные понятия. Модель нарушителя

Г. По месту действия:

- **без доступа на контролируемую территорию организации;**
- **с контролируемой территории без доступа в здания и сооружения;**
- **внутри помещений, но без доступа к техническим средствам ИС;**
- **с рабочих мест конечных пользователей (операторов) ИС;**
- **с доступом в зону данных (баз данных, архивов и т.п.);**
- **с доступом в зону управления средствами обеспечения безопасности ИС.**

1. Информационная безопасность.

Основные понятия. Проблема

До последнего времени проблема обеспечения безопасности компьютерной информации в нашей стране не только не выдвигалась на передний край, но фактически полностью игнорировалась.

Считалось, что путем тотальной секретности, различными ограничениями в сфере передачи и распространения информации, можно решить проблему обеспечения информационной безопасности.

Анализ мирового и отечественного опыта обеспечения

Информационной Безопасности диктует **необходимость создания целостной системы безопасности организации**, взаимоувязывающей правовые, организационные и программно-аппаратные меры защиты и использующей современные методы прогнозирования, анализа и моделирования ситуаций

БЛАГОДАРИЮ ЗА ВНИМАНИЕ !

ВОПРОСЫ ?

