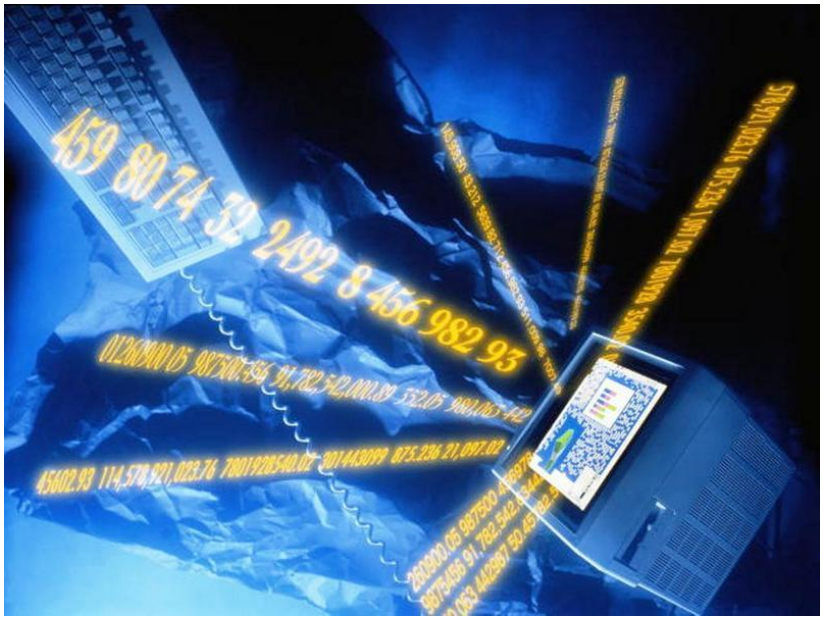
Защита информационных ресурсов государственного управления



Систематизация прав доступа:

- ***Государственная тайна*** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности

- ***Гриф секретности*** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся на их носителе, проставляемые на самом носителе и (или) в сопроводительной документации к нему;
- ***Допуск к государственной тайне*** – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну; права предприятий на проведение работ с использованием сведений, составляющих государственную тайну

- ***Доступ к сведениям, составляющим государственную тайну*** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- ***Служебная тайна*** – государственные секреты, разглашение или утрата которых может нанести ущерб национальной безопасности, обороноспособности, политическим и экономическим интересам страны

- ***Тайна переписки, телефонных переговоров и телеграфных сообщений*** относится к числу демократических свобод, а в соответствии с теорией уголовного процесса – к числу конституционных принципов уголовного процесса.
- ***Тайна личной жизни граждан –*** различного рода документированная информация ограниченного доступа, хранящаяся в государственных архивах

К сведениям, не относящимся к государственной тайне, информация о:

- Чрезвычайных происшествиях и катастрофах.
- Состоянии экологии, здравоохранении, санитарии, демографии, образования, культуры, сельского хозяйства и преступности.
- Привилегиях, компенсациях и льготах, предоставляемых государством.
- Размерах золотого запаса и государственных валютных резервах РФ.
- Фактах нарушения законности органами государственной власти и их должностными лицами.

Органы защиты государственной тайны в РФ:

- Межведомственная комиссия п защите государственной тайны;
- органы федеральной исполнительной власти: ФСБ, Министерство обороны, ФАПСИ, СВР, Государственная техническая комиссия при Президенте РФ и их органы на местах;
- Органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны

Информационная безопасность

Понятие «информационная безопасность» может рассматриваться в следующих значениях:

1. Состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система и информационная система предприятия, общества, государства и т.п.);

2. Деятельность, направленная на обеспечение защищенного состояния объекта (в этом значении чаще используется термин **«защита информации»**).

Свойства и классификация информации в управлении

- **Информация – основа процесса управления**. Без нее невозможно сформулировать цели управления, оценить ситуацию, определить проблемы, подготовить, принять решения и оценить их последствия, контролировать их выполнение.

- С точки зрения содержания и роли в управлении информация определяется как предмет труда управленческих работников и представляет собой совокупность сведений о состоянии управляемой и управляющей систем, внешней среды.

- **К основным свойствам информации**, как правило, относят:

- способность быть средством отражения процессов, событий, явлений и т. п.,
- -многократность использования,
- - при обмене информацией между двумя объектами она удваивается у каждого участника обмена,
- - свойства старения, концентрации и рассеивания.

Положение управления внутри организации зависит от его рассмотрения с одной из трёх возможных точек зрения:

- с точки зрения процессов, происходящих внутри организации;
- с позиции процессов включения организации во внешнюю среду;
- с точки зрения осуществления самой этой деятельности.

- Во внутриорганизационной жизни информационное управление играет роль координирующего начала, формирующего и приводящего в движение ресурсы организации для достижения поставленных целей путём коммуникационных процессов внутри организации,

- С целью анализа уровней информационного обеспечения процесса управления **информацию можно классифицировать по ряду признаков:**

- форме передач;
- источнику получения;
- степени свертывания;
- по типу операций и видам их обработки;
- носителям и т. д.

- **По форме передач** она может быть текстовой (письменной), устной, аудио и визуальной, кинестетической.

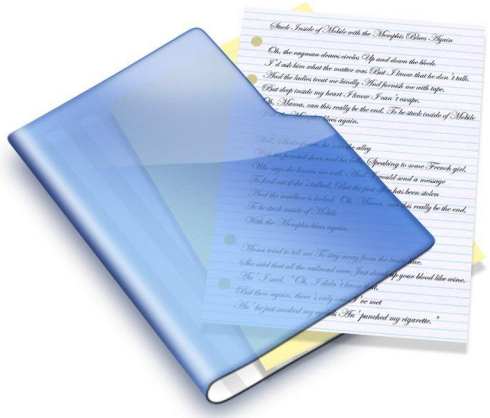
- **По источнику получения** информацию различают на первичную и вторичную.

- **По степени свертывания (обработки)** - на исходную и обработанную. Исходная получается из первичной информации, а также в результате прямых наблюдений за ходом работ учреждения. Она необходима для первичных данных. Она может являться промежуточной для более высокого уровня обобщения.

- **По типу операций** информация может быть отнесена к этапам: первичному, подготовительному и основному.

На первичном этапе осуществляется сбор данных, на подготовительном - преобразование к виду, принятому для ввода в информационный массив или канал связи, и на основном - переработка или обработка, в зависимости от назначения

Каждый из указанных типов подразделяется на классы операций.



- **Сбор** включает классы, связанные с фиксацией и передачей данных,
- **Подготовка** объединяет их приемку, редактирование и формализацию,
- **Обработка** состоит из ввода и хранения данных, переработки массивов по заданным алгоритмам и вывода информации.

- **Носители информации по типам - традиционные и нетрадиционные.**

  К носителям традиционным относятся бумажные, графические.

  К нетрадиционным - машиночитаемые, магнитные, голографические, лазерные и т. п.

- Классификация информации, используемой в процессе управления, является основной для его информационной характеристики. Она отражает формы и характер ее использования, влияние на параметры процесса управления.
- **К информационным характеристикам процесса управления относят количество и качество информации, достоверность и точность, полноту, актуальность, ценность, полезность и плотность.**

Информационные характеристики процесса управления

- **Количество информации** является основной характеристикой загрузки управленческих работников, а также производительности используемых при преобразовании информации технических средств в человеко-машинных системах. При оценке объемов информации в качестве ее единения используются понятия: символ, бит, байт, слово, знак и др.
- **Качество информации** характеризуется достоверностью, точностью, полнотой, актуальностью, ценностью, полезностью.
- **Достоверность информации** представляют числом ошибочных символов на определенный объем информационного сообщения.
- **Точность информации** характеризуется степенью соответствия реальным значениям показателей.
- **Полноту информации** определяют соотношением необходимых для процессов управления и получаемых сообщений к моменту использования;
- **Актуальность информации** во многом зависит от своевременности ее сбора, регистрации, обработки, целенаправленности и использования по назначению.
- **Ценность и полезность** характеризуются степенью ее соответствия поставленной цели, сложившейся ситуации, определенной проблеме.
- **Высокая плотность информации** определяется не только техникой ее фиксирования на носителях, но и знаками, языком ее фиксирования.

Роль информации в управленческой деятельности

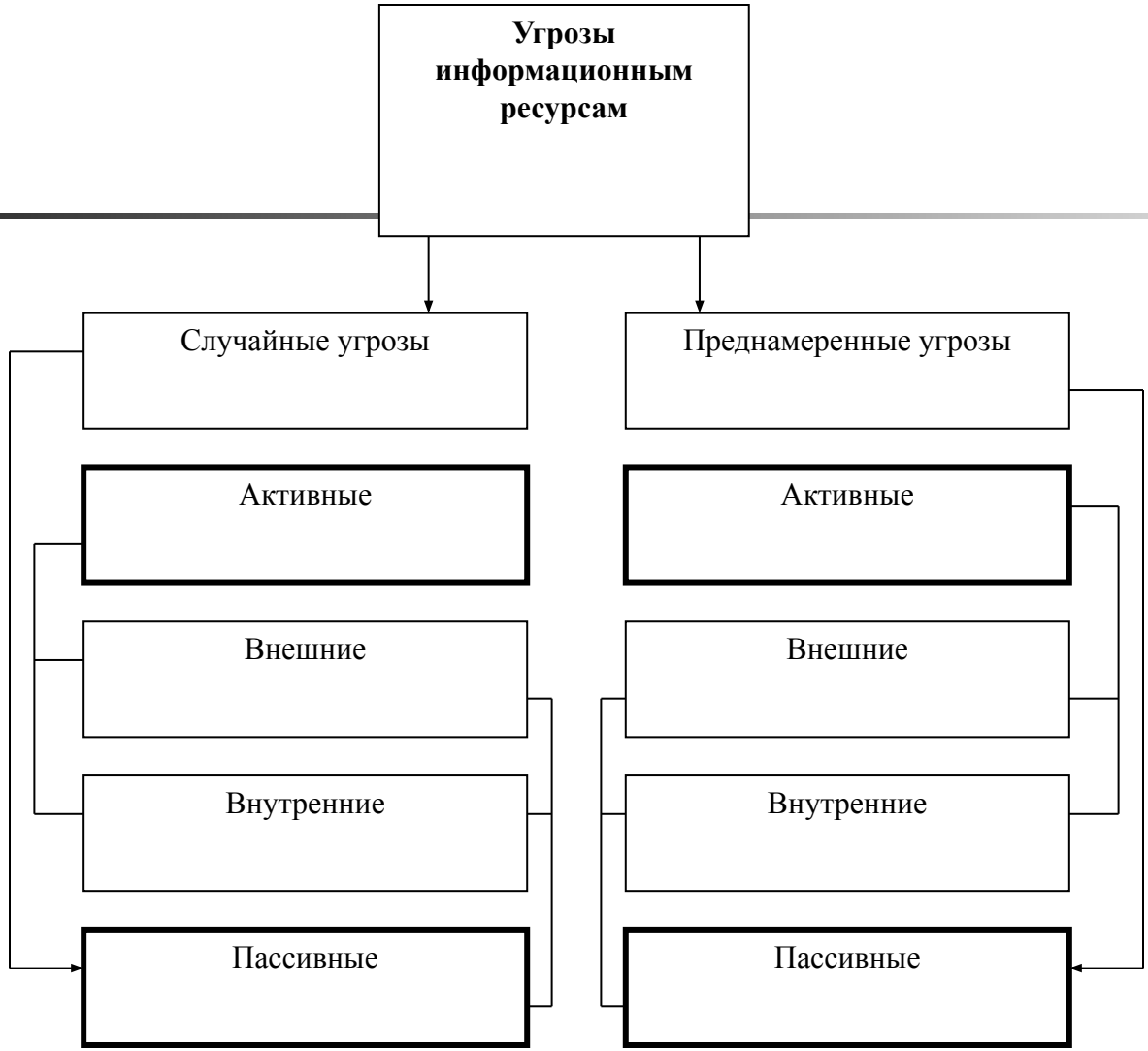
- В современных условиях используемая надлежащим образом информация может стать решающим фактором успеха в бизнесе. Информация и основанная на ней координация всех направлений деятельности отдельных подразделений организации помогает связывать их воедино во имя общей цели, принимать рациональные и адекватные данной ситуации управленческие решения и обеспечивает включение организации в изменяющуюся внешнюю среду посредством коммуникаций.
- С развитием стратегического управления и информационной экономики роль информации в современном обществе постоянно растёт: она становится не только базой для принятия решений в бизнесе, но и основным средством управленческого воздействия на работу персонала, мотивации деятельности людей.

- **Информационная безопасность** — защита конфиденциальности, целостности и доступности информации.

- **Конфиденциальность:** свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.
- **Целостность:** неизменность информации в процессе ее передачи или хранения.
- **Доступность:** свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Механизмы безопасности

- Идентификация и аутентификация;
- Управление доступом;
- Протоколирование и аудит;
- Криптография;
- Экранирование


Угрозы информационным ресурсам
Случайные угрозы
Преднамеренные угрозы
Активные
Активные
Внешние
Внешние
Внутренние
Внутренние
Пассивные
Пассивные

Причины случайных воздействий:

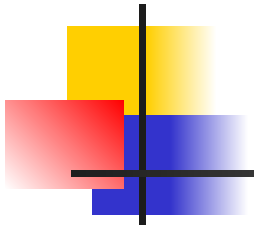
- Отказы и сбои аппаратуры;
- Помехи на линиях связи от воздействия внешней среды;
- Ошибки человека как звена информационной системы;
- Схемные и схемотехнические ошибки разработчиков аппаратуры, входящей в состав информационной системы;
- Структурные, алгоритмические и программные ошибки;
- Аварийные ситуации;
- Другие воздействия.

Преднамеренные угрозы, связанные с действиями человека:

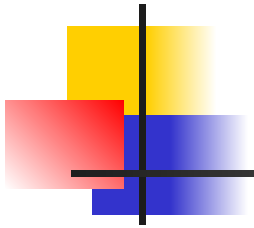
- Терминалы пользователей ИС;
- Терминал администратора ИС;
- Терминал оператора функционального контроля;
- Средства отображения информации;
- Средства документирования информации;
- Средства загрузки ПО в компьютерный комплекс;
- Носители информации;
- Внешние каналы связи (например Интернет);
- Программы со специальными логическими закладками (нелицензированные программы).

Классификация и характеристика моделей нарушителя

- **Возможные классификационные признаки моделей:**
  1. По характеру угроз
  2. По виду угроз
  3. По источнику угроз
  4. По объекту угроз
  5. По топологии
  6. По признаку воздействия на статус информационного ресурса



7. По типу модели: формализованные и не формализованные;
8. По назначению: исследовательские, учебные, проектные;
9. По сложности: комплексные, частные;
10. По виду используемого математического аппарата: графовые, вероятностные, на основе теории массового обслуживания



- Моделирование процессов нарушения информационной безопасности целесообразно осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации угрозы – уязвимость – последствия»

ТРЕБОВАНИЯ К МОДЕЛИ НАРУШИТЕЛЯ

- Служба безопасности должна построить модель типичного злоумышленника.
- Необходимо оценить, от кого защищаться в первую очередь. Опираясь на построенную модель злоумышленника, можно строить адекватную систему информационной защиты.
- Правильно разработанная модель нарушителя является гарантией построения адекватной защиты.

ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

- Система защиты информации должна быть адекватной уровню важности, секретности и критичности защищаемой информации.
- Ее стоимость не должна превосходить возможный ущерб от нарушения безопасности охраняемой информации.
- Преодоление системы защиты должно быть экономически нецелесообразно по сравнению с возможной выгодой от получения доступа, уничтожения, модификации или блокировки защищаемой информации.
- Для достижения поставленных целей нарушитель должен приложить определенные усилия и затратить некоторые ресурсы.

Особенности построения модели нарушителя

Для построения модели нарушителя используется информация от служб безопасности и аналитических групп:

- о существующих средствах доступа к информации и ее обработки,
- о возможных способах перехвата данных на стадии передачи, обработки и хранении,
- об обстановке в коллективе и на объекте защиты,
- сведения о конкурентах и ситуации на рынке,
- об имевших место свершившихся случаях хищения информации.

ТИПЫ НАРУШИТЕЛЕЙ

- **Хакер-одиночка**, обладающий стандартным персональным компьютером, с модемным (реже выделенным) выходом в Интернет. Данный тип злоумышленников очень сильно ограничен в финансовом плане.
- Он необязательно обладает глубокими знаниями в области компьютерных технологий, чаще всего использует готовые компьютерные программы, доступные из Интернета, для реализации угроз через давно известные уязвимости.

- **Объединенная хакерская группа**. Исследуемый тип злоумышленников достаточно скован в своих финансовых возможностях. Она еще не обладает вычислительными мощностями уровня крупного предприятия и подобным пропускным каналом в Интернет. Но обладание суммарными знаниями в области компьютерных технологий представляют большую опасность. Такие злоумышленники используют всевозможные приемы для организации сканирования информационных систем с целью выявления новых уязвимостей, применяются также методы реализации угроз через уже известные уязвимости.

Организация - конкурент

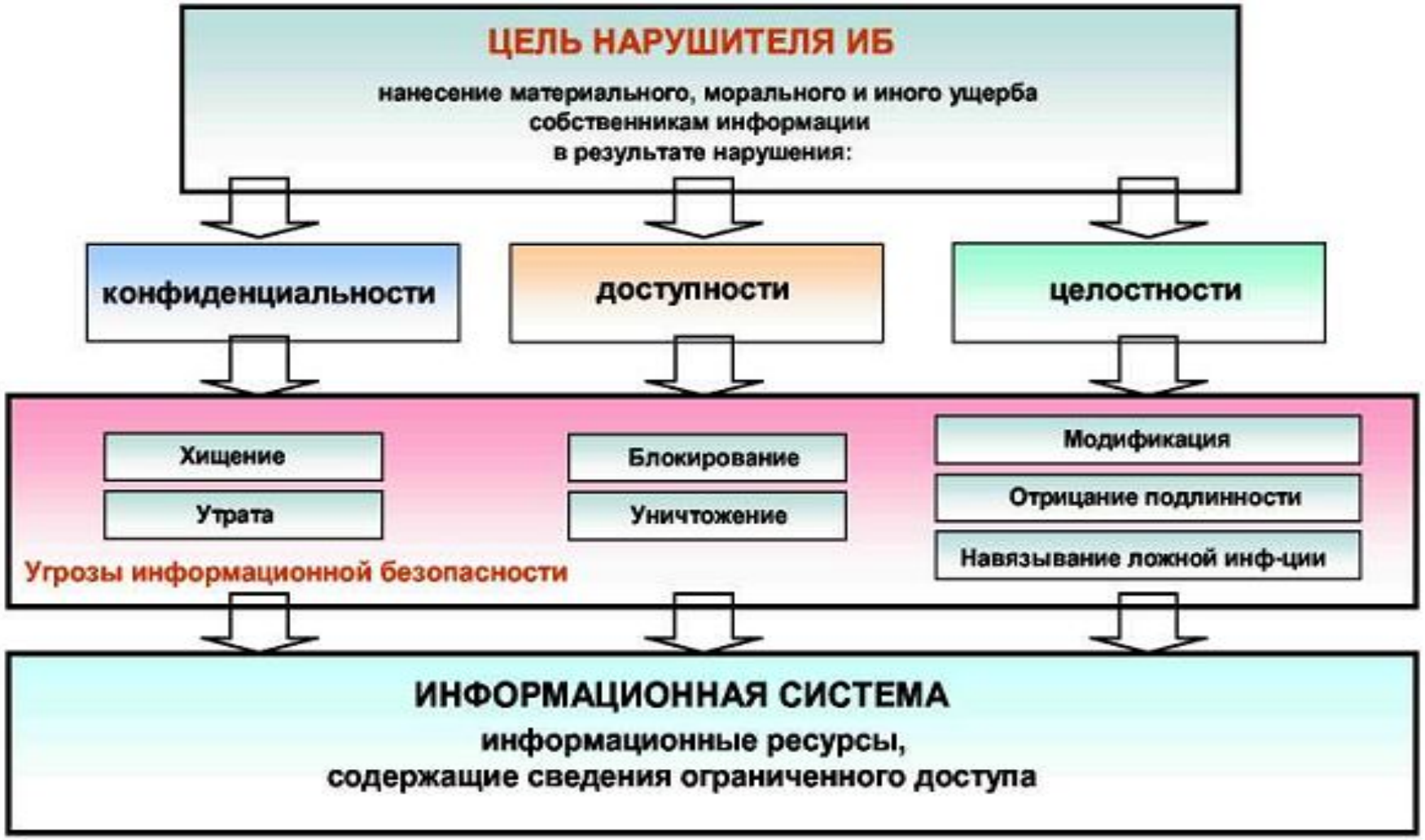
- Данная модель включает в себя:
- собственные мощные вычислительные сети и каналы передачи данных с высокой пропускной способностью для выхода в Интернет;
- большие финансовые возможности;
- высокие знания компьютерных специалистов как самой компании, так и нанимаемых "под заказ".
- возможны попытки подкупа сотрудников службы безопасности или иные действия из области социальной инженерии.

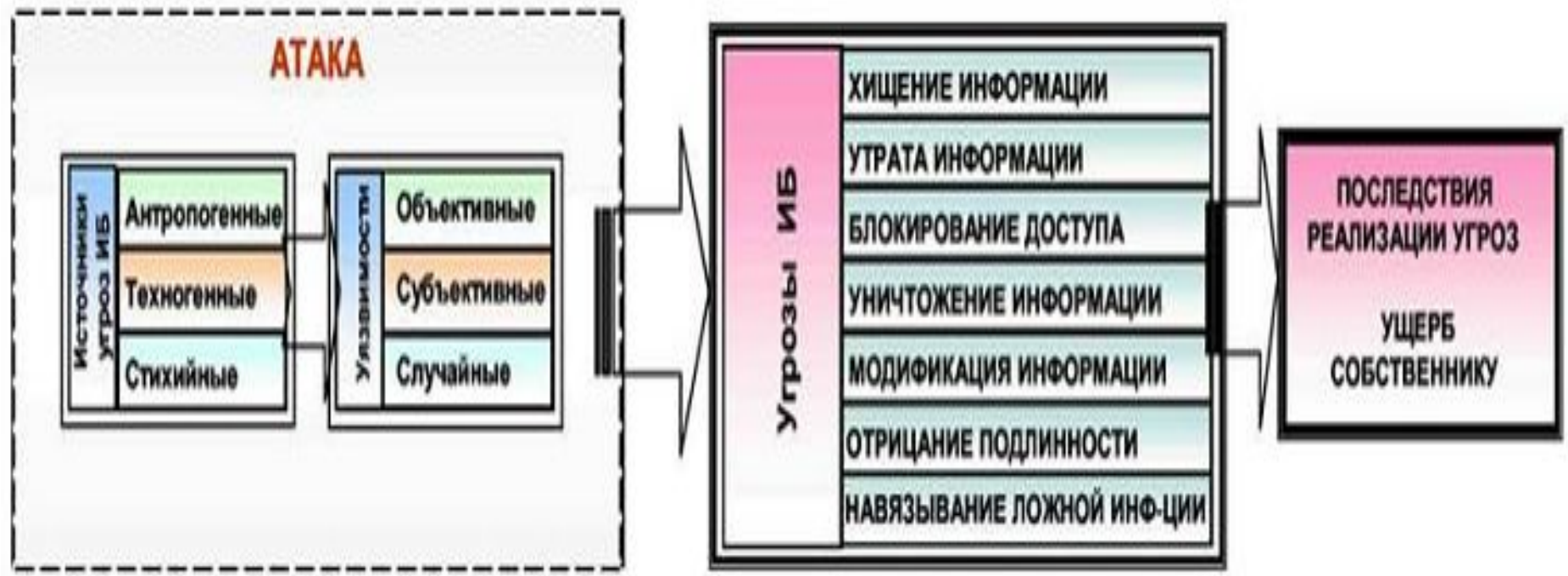
Коррумпированные представители различных структур ведомственного уровня, а также спецслужбы различных государств.

Они обладают практически неограниченными вычислительными и финансовыми возможностями, самостоятельно регулируют и контролируют трафик в сети Интернет.

На их службе состоят самые высокопрофессиональные компьютерные специалисты.

В некоторых странах известны примеры, когда вместо тюремного заключения или после него известного хакера берут в службу национальной безопасности.


ЦЕЛЬ НАРУШИТЕЛЯ ИБ
нанесение материального, морального и иного ущерба собственникам информации в результате нарушения:
конфиденциальности
доступности
целостности
Хищение
Утрата
Блокирование
Уничтожение
Модификация
Отрицание подлинности
Навязывание ложной инф-ции
Угрозы информационной безопасности
ИНФОРМАЦИОННАЯ СИСТЕМА
информационные ресурсы, содержащие сведения ограниченного доступа


АТАКА
Источники угроз ИБ
Антропогенные
Техногенные
Стихийные
Уязвимости
Объективные
Субъективные
Случайные
Угрозы ИБ
ХИЩЕНИЕ ИНФОРМАЦИИ
УТРАТА ИНФОРМАЦИИ
БЛОКИРОВАНИЕ ДОСТУПА
УНИЧТОЖЕНИЕ ИНФОРМАЦИИ
МОДИФИКАЦИЯ ИНФОРМАЦИИ
ОТРИЦАНИЕ ПОДЛИННОСТИ
НАВЯЗЫВАНИЕ ЛОЖНОЙ ИНФ-ЦИИ
ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ
УЩЕРБ СОБСТВЕННИКУ

Организационно-технические и режимные меры и методы

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая Политика информационной безопасности.

Политика безопасности (информации в организации) — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

- Определение информационных и технических ресурсов, подлежащих защите;
- Выявление полного множества потенциально возможных угроз и каналов утечки информации;
- Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- Определение требований к системе защиты;
- Осуществление выбора средств защиты информации и их характеристик;
- Внедрение и организация использования выбранных мер, способов и средств защиты;
- Осуществление контроля целостности и управление системой защиты.

Организационная защита объектов информатизации

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает:

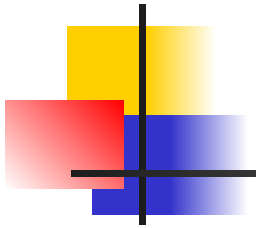
- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.
- К основным организационным мероприятиям можно отнести:
- организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Но в условиях современного общества защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;

Безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

ЗАКЛЮЧЕНИЕ



Из рассмотренного становится очевидно, что обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Для решения проблемы обеспечения информационной безопасности необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.