Основы Защиты Информации

**Основные понятия и определения в сфере защиты информации (ЗИ)**

**Информация:**

* Обозначение содержания, полученного от внешнего мира в процессе приспособления к нему (Винер);
* Коммуникация и связь, в процессе которой устраняется неопределенность (Шеннон);
* Мера сложности структур (Моль);
* Сведения о лицах, предметах, фактах событиях и процессах независимо от формы их представления

(Закон РБ об информации, информатизации и защите информации).

Информация может существовать в виде бумажного документа, физических полей и сигналов, в памяти человека.

*В дальнейшем будем рассматривать информацию:*

в документированной форме (на бумаге);

в форме физических полей (радио, акустических).

**Информационный объект (ИО)** – среда в которой информация создается, передается, обрабатывается или хранится.

**Угроза** – возможные воздействия на ИО приводящие к ущербу.

**Уязвимость** – свойство ИО делающее возможным возникновение и реализацию угрозы.

**Комплексная защита ПО** – совокупность методов и средств.

**Безопасность информационного объекта** – его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

**Защищенный ИО** – объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

**Виды ущерба ИО или поддерживающей инфраструктуре:**

– Нарушение конфиденциальности - несанкционированный доступ к информации, нарушение свойства инф. быть известной только определенным субъектам;

– Нарушение целостности - несанкционированное изменение или уничтожение информации;

– Нарушение доступности (возможность за приемлемое время получить требуемую информационную услугу, отказ в обслуживании) - нарушение доступа к информации, работоспособности объекта;

– Нарушение права собственности на информацию.

**Классификация угроз:**

*По виду ущерба:*

(доступность, целостность, конфиденциальность, право собственности);

*По компонентам информационных систем на которые угрозы нацелены:*

(данные, программы, аппаратура, поддерживающая инфраструктура);

*По источникам:*

(люди, технические устройства, программы, внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки));

*По происхождению:*

(случайные, преднамеренные, природные/техногенного характера);

*По расположению источника угроз:*

(внутренние/внешние).

**ЗИ от случайных угроз:**

* Дублирование информации;
* Оптимизация взаимодействия человека и системы;
* Блокировка ошибочных операций;
* Создание отказоустойчивых систем;
* Повышение надежности;
* Минимизация ущерба от аварий и бедствий.

**Социальная инженерия** – манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации (в отличие от социального программирования, которое применяется не только для взлома, используется и для других целей: обуздание толпы, победы на выборах, и т.д. и реализуется без использования ЭВМ).

Человек понимается как часть компьютерной системы.

**Соц. инженерия** - хакерство с использованием человеческого фактора.

**Роль человеческого фактора в ЗИ:**

Взлом систем ЗИ от несанкционированного доступа систем охранной сигнализации и т.д. в 80% случаев происходят из-за человеческого фактора.

**Психологические предпосылки** (схема Шейнова В,П.)**:**

* Формирование цели воздействия на объект;
* Сбор информации об объекте воздействия;
* Обнаружение наиболее удобных мишеней воздействия;
* Аттракция (от лат. привлекать, притягивать) - создание нужных условий для воздействия на объект;
* Принуждение к нужному действию;
* Нужный итог.

**Обратная соц. инженерия** - создание условий при которых объект сам просит вас прийти.

* **Проблема "уборщицы":**

Низкая проверка при трудоустройстве + доступ в места, в которые нет почти ни у кого.

* **Выставки и презентации:**

Проблема - наказание за кражу БД предприятия - практически никакой;

В судах практически нет обращений от организаций, у которых крадут инфу.

**Правило 1.**

Ни один из сотрудников предприятия не должен знать больше, чем ему полагается знать по должности (подавляющее большинство людей не могут хранить секреты).

**Правило 2.**

В трудовом контракте обязательно должен быть пункт об ответственности сотрудника, вплоть до уголовной.

**Области применения соц. инженерии:**

Финансовые махинации (Наташа + Илья = ..);

Конкурентная разведка:

* Информация о маркетинговых планах организации (выставки, интервью с ключевыми лицами и т д ) см правила 1 и 2;
* Воровство клиентских баз данных - правила 1 и 2 + доступ в офис и серверам;
* Информация о наиболее перспективных сотрудниках;
* Информация об организации с целью последующего уничтожения конкурента.

**Области применения соц. инженерии:**

* Фишинг и другие способы кражи паролей с целью доступа к персональным банковским данным частных лиц (защита: генерация одноразовых паролей/ использование USB устройств/ мобильное подтверждение/ хеширование паролей);

* Фарминг - изменение адресов так, чтобы страницы, которые посещает пользователь были не оригинальными, а фишинг-страницами;

* Общая дестабилизация работы организации;

* Рейдерские атаки.

(методы соц. инженерии применяются на первом этапе сбора информации)

**Настройка "человеческого брандмауэра"** - постоянная работа;

"безопасность - это *процесс*".

Защита информации должна быть *системной.*

**Информационная безопасность:**

защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре.

**Защита информации:**

комплекс правовых организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации

(*(Закон РБ "о информации информатизации и защите информации*").

**Классификация методов защиты информации**

**Методы ЗИ:**

1. Законодательные (правовые);
2. Организационные;
3. Технические (в т.ч. программные);
4. (1 + 2 + 3 = 4) комплексные.

**К объектам информационной безопасности относятся:**

* Личность - ее права и свободы;
* Общество - его материальные и духовные ценности;
* Государство - его конституционный строй;
* Суверенитет и территориальная целостность.

**Субъекты обеспечения информационной безопасности:**

* Государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти;
* Юридические лица;
* Граждане обладающие в соответствии с законодательством правами и обязанностями по участию в обеспечении государства.

В качестве обоснования выбора средств защиты (организационных и программно-технических) могут выступать результаты анализа риска и статистика, накопленная по инцидентам. Механизмы реализации анализа риска и накопления статистики должны быть отражены в политике безопасности компании.

**Политика безопасности:**

совокупность норм и правил, регламентирующих работу средств защиты информационного объекта от заданного множества угроз безопасности.

К наиболее дешевым (однако имеющим высокий уровень эффективности) относятся *организационные меры* (внутренний и внешний аудит. Анализ риска, политика информационной безопасности).

**Охраняемые сведения и демаскирующие признаки**

***Категории доступа* информации:**

* Общедоступную;
* Информацию, распространение и (или) предоставление которой ограничено;
* Информация о частной жизни физ. лица и персональные данные;
* Сведения, составляющие государственные секреты;
* Информация, составляющая коммерческую тайну;
* Информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда \*до завершения производства по делу

(*Закон "об информации, информатизации и защите информации"*).

**Охраняемые сведения и демаскирующие признаки**

**Охраняемые сведения:**

Сведения, содержащие гос. секреты или отнесенные к другой категории конфиденциальной информации.

**Государственные секреты:**

Защищаемые государством сведения, распространение которых может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам РБ.

* Государственная тайна;
* Служебная тайна.

**Государственная тайна:**

Сведения, в результате разглашения или утраты которых могут наступить **тяжкие последствия** для нац. безопасности РБ.

**Служебная тайна:**

Сведения, в результате разглашения или утраты которых может быть причинен **существенный вред** нац. безопасности РБ.

**Гриф секретности:**

Реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов.

**На носителях государственных секретов проставляются следующие грифы секретности:**

На носителях государственной тайны и (или) сопроводительной документации к ним - "Особой важности", "Совершенно секретно";

На носителях служебной тайны и (или) сопроводительной документации к ним - "Секретно".

**Формы доступа к государственным секретам:**

Форма №1 - форма допуска к *государственной* тайне, имеющей степень секретности "Особой важности";

Форма №2 - форма допуска к *государственной* тайне, имеющей степень секретности "Совершенно секретно";

Форма №3 - форма допуска к *служебной* тайне, имеющей степень секретности "Секретно".

**Демаскирующие признаки (ДП):**

любые характеристики, которые можно обнаружить с помощью разведывательной аппаратуры, проанализировать и получить информацию об охраняемых сведениях.

Первичные - непосредственно регистрируются аппаратурой;

Вторичные - накоплением и обработкой первичных демаскирующие признаки.

Развитие информационных технологий создает качественно новые угрозы, способные приводить порой к катастрофическим масштабам последствиям.

**Обеспечение информационной безопасности** - это непрерывный процесс.

Безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах и на всех этапах обработки информации.

**История развития методологии информационной безопасности**

**1983 - "Критерии оценки доверенных компьютерных систем"** (США), или "Оранжевая книга";

**"Красная книга"** - инструкция Национального центра компьютерной безопасности;

**"Зеленая книга"** - разработано агентством информационной безопасности ФРГ;

**"Белая книга"/"Критерий оценки защищенности ИТ"** - Европейский стандарт (на базе ЗК).

**Общие критерии Common Criteria:**

Разрабатывали США, Британия, Франция, Канада и т.д.;

1 версия 1996;

В качестве стандарта принята версия 2.0 1999г

"Общая методология оценки безопасности ИТ".

**ISO/IEC 15408** - международный стандарт информационной безопасности.

Возникла реальная перспектива создания *единого безопасного информационного пространства,* в котором сертификация безопасности систем обработки информации будет глобальной.

Цель: Упростить, удешевить, ускорить выход сертифицированных изделий ИТ на мировой рынок за счет взаимного признания сертификатов.

**СТБ 34.101.х -2014, BY**

"Информационные технологии и безопасность. Критерии оценки безопасности ИТ".

**Правовые методы защиты информации**

Разработка и совершенствование законодательной базы информационной безопасности является необходимой мерой, удовлетворяющей потребность в защите информации при развитии социально-экономических, политических, военных направлений деятельности каждого государство.

**Правовое обеспечение ЗИ:**

* Нормотворческая деятельность -

Создание законодательства в области информационной безопасности;

* Исполнительная и правоприменительная деятельность -

По исполнению законодательства в области информации, информатизации, защите информации органами государственной власти и управления, организациями, гражданами.

**Основные принципы деятельности по правовому обеспечению информационной безопасности:**

* Соблюдение законности -

Создание законов их применение и исполнение;

* Обеспечение баланса интересов отдельных субъектов и государства -

Предусматривает приоритет государственных интересов как общих интересов всех субъектов;

* Неотвратимость наказания -

Важнейший профилактический инструмент.

**Нормативные документы:**

* Общегосударственные:
  + Законы, кодексы;
  + Указы президента РБ;
  + Постановления Совета Министерства.
* Ведомственные:
  + Межведомственные;
  + Внутриведомственные.

**Основные законы**

* **Основной закон государства - Конституция РБ.**

Гражданам РБ гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации.

Пользование информацией может быть ограничено государством с целью защиты прав и свобод граждан.

* **Гражданский кодекс РБ.**

Электронная подпись признается.

Ответственность за незаконное использование информации.

* **Уголовный кодекс РБ (УК РБ).**

**Закрепляется ответственность:**

* ст. 212;
* ст. 373;
* ст. 374;
* ст. 375;
* и т.д..

* **Кодекс РБ об административных правонарушениях:**
  + ст. 9.6 - отказ в предоставлении информации;
  + ст. 22.6 - несанкционированный доступ к компьютерной информации;
  + ст. 22.7 - нарушение правил ЗИ.

**Трудовой кодекс РБ:**

Для работников - хранить государственную и служебную тайну, не разглашать коммерческую тайну и т.д..

**Налоговый кодекс РБ**

**Нормативные документы**

**Общегосударственные документы:**

* Законы, кодексы;
* Указы президента РБ;
* Постановления Совета Министров;
* Ведомственные документы;
* Межведомственные документы;
* Внутриведомственные документы.

* Закон "Об информации, информатизации и защите информации" 10 ноября 2008 г. №455-3:
* Изменения и дополнения от 4 января 2014 г. № 102-3;
* Изменения и дополнения 11 мая 2016 г. №362-3.

**Информационная сеть:**

Совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих путем сетей электросвязи.

**Информационная система:**

Совокупность банков данных и т.д..

**Конфиденциальность информации:**

Требование не допускать распространение и (или) предоставление информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами РБ.

*Действие настоящего Закона не распространяется на общественные отношения, связанные с деятельностью СМИ и охраной информации, являющиеся объектами интеллектуальной собственности.*

**Основные принципы правового регулирования информационных отношений:**

* Свободы пользования информацией (в рамках закона);
* Установление ограничений на распределение и/или предоставление информации только законодательными системами РБ;
* Своевременность предоставления;
* Защита информации о частной жизни физических лиц и персональных данных;
* Обеспечение безопасности личности, общества и государства.

**Статья 6 Право на информацию:**

Не может быть использовано для противоправных деяний.

Глава2. Государственное регулирование и управление в области информации, информатизации и ЗИ

**Включает что-то там:**

* Техническое нормирования и стандартизация;
* Формирование единой политики в этой области;
* Привлечение инвестиций;
* Международное сотрудничество;
* Усовершенствованное законодательство.

**Осуществляется**

* Президентом РБ;
* Советом Министров РБ;
* НАН РБ;
* Оперативно-аналитическим центром при Президенте РБ;
* Министерством связи и информатизации РБ;
* Иными гос. органами в пределах их компетенции.

Статья 16 Общедоступная информация

**Не могут быть ограничены доступ и предоставление информации:**

* О правах и свободах;
* О правовом статусе государственных органов;
* О ЧС, экологической, санитарно-эпидемиологической обстановке и т.д.;
* О преступности, демографии;
* О льготах и компенсациях;
* О золотом запасе;
* О внешних задолженностях;
* …

Оперативно-аналитический центр (ОАЦ)

Сначала он был ГЦБИ (государственный центр БИ), изначально в подчинении Совету Безопасности РБ, а потом президенту (в 2004)

**ОАЦ**- государственный год

**Подчиненные организации:**

* НИИТЗИ;
* НЦОТ;
* НЦЭУ.

Государственный реестр информационных ресурсов

Государственная регистрация осуществляется Министерством связи и информатизации РБ

Статья 27 Цели защиты информации

**Меры по защите информации**

* Правовые
* Организационные
* Технические

Закон "Об электронном документе и электронной цифровой подписи"

28.12.2009

Белорусский стандарт ЭЦП

Закон "Об органах государственной безопасности РБ"

10.07.2012

Указ "Об утверждении концепции национальной безопасности РБ"

09.11.2010

**Основные понятия**

* **Национальная безопасность:**

Состояние защищенности национальных интересов РБ от внутренних и внешних угроз.

* Политическая безопасность;
* Экономическая безопасность;
* Социальная безопасность;
* Демографическая безопасность;
* Научно-технологическая безопасность;
* Военная безопасность;
* Экологическая безопасность.

Указ "О мерах по совершенствованию использования нац. сегмента сети Интернет"

01.02.2010

Указ " О некоторых мерах по обеспечению безопасности критически важных объектов информации"

**КВОИ:**

Объект информатизации, который обеспечивает ф-ние экологически опасных и/или социально значимых производств и технологических процессов, нарушение штатного режима которых, может привести к чрезвычайной ситуации техногенного характера.

**Организационные методы ЗИ**

Проводятся

* Государством
* Собственность информации

В общегосударственных системах и сетях

* **Аттестация** объектов информатизации
* **Сертификация** средств защиты
* **Лицензирование деятельности**
* **Введение** территориальных, частотных, пространственных и временных **ограничений**
* Создание и применение **защищенных** информационных и автоматизирующих систем управления

**Техническое нормирование и стандартизация в области информационной безопасности**

В "Оранжевой книге" заложен понятийный базис информационной безопасности

Введены понятия

* Безопасная и доверенная система
* Ядро безопасности и периметр безопасности
* ..

В ОК определены 7 уровней безопасности

СТБ 34.101.х -2014 BY

Информационные технологии и безопасность. Критерии безопасности информационных технологий

Устанавливаются требования к средствам ЗИ с целью защиты жизни и здоровья человека, а также для предотвращения действий, вводящих в заблуждения

СТБ 34.101.8 - 2006, BY

Информационные технологии. Методы и средства безопасности ПС защиты от воздействий вредоносных программ и антивирусные ПС

Стандарт не распространяется на АС аппаратные средства

**Технические каналы утечки информации**

Средства передачи информации

Физически:

* Звуковые волны
* Материалы и вещества
* Световые лучи
* Электромагнитные волны

Каналы утечки информации по физическим принципам:

* Акустический (1)
  + Прямой
  + Акустоэлектрический
  + Акустооптический
  + Параметрический
* Материально-вещественный (2)
  + Хищение
  + Копирование
  + Ознакомление
* Визуально-оптический (3)
  + Наблюдение
  + Съемка
* Электро-какой-то (4)
  + Электрический
  + Индукционный
  + Параметрический (электромагнитный)

Закладное устройство ::=

Устройство, объединяющие микрофон и передатчик (жучок)

1.3 Возникает за счет преобразований акустических сигналов в электрические

* Индуктивные
* Емкостные
* Пьезоэлектрические
* Магнитокакие-то

Применяются в

* Электромеханических звонках
* Отдельных типах электромеханических реле
* Громкоговорителях
* Некоторых типах датчиков охранной и пожарной сигнализации

Микрофонный эффект в звонках проявляется даже при положительной трубке

1.4 Исп. Оборудование с лазером, луч которого направляется в помещение, где ведутся переговоры, отражается, его принимают злоумышленники

По физическому состоянию:

* Твердые массы
* Жидкости
* Газообразные вещества

По физической природе

* Химические
* Биохимические
* Радиоактивные

По сфере распространение

* По земле
* По воздуху
* По воде

4 Носители информации - электромагнитные волны и электрический ток

Электрический канал

Автоматически созданный замещающий текст:
Источник 
конфеденциальной 
информации 
Источник 
фоновых э/м 
шумов 
Среда 
распространения 
Проводная 
линия 
Средство тех. 
разработок 

4 3 Параметры

Пере(..)енные э/м поля имеют параметры, отличные от об(..)аемого

Источник образования технических каналов утечки информации

* Акустоэлектрические преобразователи
  + Индуктивные
  + Емкостные
  + Пьезоэлектрические
  + Магнитностри(..)ционные

* Паразитные связи
* Нежелательные улучшения технических средств обработки информации (ТСПИ)
* Утечка информации по цепям заземления
* Утечка информации по цепям электропитания
* Утечка информации в волоконно-оптических линиях связи
* Высокочастотные навязывание
* Перехват информации в телефонных каналах связи

Нежелательные улучшения

Для ПК потенциально-информационными ПЭМИ являются улучшения, формируемыми

* Цепями, по которым передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате
* По которым передается видеосигнал от видеоадаптера к монитору
* Формирующие шину данных сист. Шину и др.

По цепям заземления

Причины:

* Наличие э/м поля в местах расположения элементов заземления
* Проникновение опасного сигнала в цепи заземления может быть связано с образованием контуров заземления
* Земля - отличный проводник

Э/м поле опасного сигнала в грунте вокруг заземлителя

Высокочастотные навязывания

* Посредством контактного введения высокочастотного сигнала эл. Цепи
* Облучение ТСОИ высокочастотным э/м полем

**Криптографические методы ЗИ**

Криптография ::=

Совокупность методов преобразования информации, направленных на то, чтобы сделать ее бесполезной для недоброжелателей

Методы:

* Подстановка
* Перестановка
* Аналитические преобразования
* (..)ирование
* Комбинирование

ГОСТ 28147-489

ЭЦП ::=

Реквизит документа, предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ЭЦП, позволяющий идентифицировать владельца, установить отсутствие исчисления в документе

СТБ 1176.1-99

СТБ 1176.2-99

СТБ 34.101.31

СТБ 34.101.45

СТБ 34.101.47

СТБ 34.101.60

СТБ 34.101.66

СТБ 34.101.77

Аутентификация ::=

Определение личности обращающейся стороны

Авторизация ::=

Разрешение доступа к ресурсу

Аутентификация

* По уникальной цифре (пароль/ PIN)
* По уникальному предмету (ключ/ паспорт)
* По биометрическим параметрам
  + Статические (физиологические)
  + Динамические (поведенческие)
    - Почерк
    - Голос
    - Походка
    - Клавиатурный почерк

Идентификация ::=

Сравнение предъявленных параметров со всеми записями из базы зарегистрированных пользователей

Верификация ::=

Сравнение с единственной записью из базы

Свойства биометрических параметров :

* Всеобщность (каждый человек имеет биометрические характеристики)
* Уникальность
* Постоянство (должны быть стабильны во времени)
* Измеримость
* Применимость (общество и пользователи не должны возражать против сборов биом. п-ра)

Требования к системе ЗИ основанной на биометрических параметрах

* Точность
* Скорость вычисления и возможность масштабирования БД
* Обработка исключительных случаев
* Стоимость
* Конфиденциальность
* Безопасность

Биометрическая аутентификация не дает 100% результата

**Функции системы разграниченного доступа:**

* Разграничение доступа к данным
* РПД и у(..) создания твердых копий
* ..

Субъект ::=

Пользователи и процессы

Объекты ::=

Информация и другие ресурсы

Задача логического управления доступом в разграничении прав для каждой пары субъект-объект

Методы разграничения доступа:

* По спискам
* С использованием матрицы установления полномочий
* По уравнениям секретности и категориям
* Парольная

**Вирус** ::=

Программа, способная создавать свои копии и внедрять их без ведома пользователей

Вирусы:

По среде обитания

* Файловые
* Загрузочные
* Файлово-загрузочные
* Сетевые
* Макро-вирусы

По способу заражения:

* Рецедентный (делает копии)
* Нерезедентный

По степени воздействия

* Не опасные
* Опасные
* Очень опасные

По особенностям алгоритма работы

* Полиморфные
* Стелс-вирусы
* Трояны
* Сетевые черви
* Программные закладки

**Защита**

* Антивирусные программы
* Программы-детекторы
* Доктора
* Ревизоры
* Вакцины
* Фильтры
* Сканеры
* Маски

Межсетевые экраны Firewall - устройства контроля доступа в сеть, предназначенные для блокирования всего трафика за исключением разрешенных данных.

Виртуальные частные сети

+ Нет необходимости в строительстве

+ Нет необходимости в покупке, защите и поддержке ИТ-оборудования

+ Работа лучших ИТ-специалистов 24/7

+ Обмен опытом между специалистами

Инженерно-технологические методы ЗИ

Функции

* Предотвращение и нейтрализация преднамеренных и случайных воздействий на источник информации
* Скрытие информации и ее носителей от злоумышленников на всех этапах ЖЦ (жизненного цикла) информациии
* Обнаружение и нейтрализация всех видов и средств перехвата информации

Виды:

* Физическая
  + Инженерная
  + Техническая
* Скрытие информации
  + Пространственное
  + Структурное
  + Временное
  + Энергетическое

Нейтрализация источников опасных сигналов

Физическая защита ::=

Затруднение продвижения источников угроз и источником информации

Инженерная ::=

Естественные и искусственные преграды

Техническая ::=

Методы обнаружения вторжений в контролируемые зоны и их нейтрализация

Скрытие информации ::=

Объединяет группу методов ЗИ, основу кот. составляют условия и действия затрудняющие поиски и обнаружение объекта защиты, распознавание и измерение их признаков, перехват с носителей информации с качеством, достаточным для ее использования

Пространственные ::=

Затрудняет поиск и обнаружение источников информации в пространстве. Достигается размещением источника в скрытом месте

Структурные ::=

Изменение или создание ложного информационного портрета семантического сообщения, физического объекта или сигнала

Информационный портрет ::=

Совокупность элементов и связей между ними отображающих смысл сообщения, объекта или сигнала.

Способы изменения информационного портрета:

* Удаление части элементов и связей, образующих информационный узел
* Изменение части элементов информационного портрета
* Удаление и изменение

Информационные узлы ::=

Наиболее информативные признаки и сведения

Маскировка ::=

Структурное скрытие, в результате которого информационный портрет изменяется под информационный портрет фона

Дезинформирование ::=

Трансформация исходного информационного портрета в новый, соответствующий ложной семантической информации.

Временное скрытие ::=

Значительное уменьшение времени передачи информации по канальной связи

Механические системы защиты

* Система охраны периметра
* Жалюзи/ роллеты и др.

**Социальная инженерия** ::=

Манипулирование человеком или группой людей с целью взлома системы безопасности и похищения важной информации

Психологические предпосылки (схема Шейнова В.П)

* Формирование цели воздействия на объект
* Сбор информации об объекте воздействия
* Обнаружение наиболее удобных методов воздействия
* Аттракция

Создание нужных условий для воздействия на объект

* Принуждение к нужному действию
* Нужный итог

Области применения социальной инженерии

* Финансовые махинации
* Конкурентная разведка
* Фишинг и другие способы чего-то
* Фарминг - изменение страниц так, чтобы они принимали вид оригинальных. Вляясь фишиноговыми
* Общая дестабилизация работы
* Рейдерские атаки

**Интеллектуальная собственность**

Объект ИС ::=

Материализованный результат нематериального по своей природе мыслительного процесса

На этот материализованный результат автор получает исключительное право

Всемирная организация интеллектуальной собственности (штаб-квартира в Женеве)

Интеллектуальная собственность:

* Авторское право и смежные права
* Объекты права промышленной собственности

Произведения литературные, драматические, хореографические, музыкальные с текстом и без текста.

Произведения изобразительного искусства, прикладного искусства и дизайн

Фотографии, карты, планы и пластические произведения, отнсящиеся к географии  
и др.

Объекты смежных прав:

* Исполнение
* Фонограммы
* Передача вещания

Субъект - автор

Объекты прав промышленной собственности :

Технико-конструкторские решения;

Средства индивидуализации участников гражданского оборота товаров, работ, услуг;

Секреты производства;

Рациональные предложения

Статут Анны 1709 г.

Субъект права промышленной собственности - изобретатель

**Основные положения об авторских правах**

Авторские права (АП) распространяются как на обнародованные, так и на необнародованные произведения

(совокупность полномочий автора, закрепленные законом)

Авторское право не распространяется на

* Идеи
* Методы, процессы, системы, способы, концепции, принципы, открытия, факты

Произведения должны быть творческими

Личные неимущественные права:

(сохраняются независимо от имущественных)

* Право на авторство
* Право на имя
* Право на обнародование
* Право на защиту репутации автора

Не охраняются авторские АП:

* Официальные документы и перевод
* Государственные символы и знаки
* Произведения народного творчества

АП возникают в силу факта создания произведения и не требуют регистрации

© - copyrigh - знак охраны АП

АП:

* Личные неимущественные
* Имущественные

Имущественные:

* Воспроизведение
* Распространение
* Прокат
* Публичный показ
* Передача в эфир
* Перевод
* Переделка или иная переработка

Соавторское произведение принадлежит соавторам совместно

Ограничение имущественных прав :

Использование произведения без согласия автора и без выплаты автору вознаграждения

Срок действия АП

на неимущественные сохраняется бессрочно

Имущественные действуют в течение жизни автора (хотя бы одного из соавторов) и 50 лет после смерти

АП может переходить по наследству, кроме прав авторства, имени и права на защиту репутации

Смежные права (СП)

Возникают при приобретении имущественных авторских прав на основе заключения договоров с авторами и наследниками

Субъекты СП:

* Исполнители
* Фонограмма
* Эфир

Имущественные права могут быть уступлены полностью или частично

Промышленная собственность

Исключительные права на объекты промышленной собственности

Исключительные права возникают не по факту создания объекта, а в связи с регистрацией объекта в государственной структуре

Охранный документ ::=

Выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объекты промышленной собственности и исключительное право на его использование

Изобретение ::=

Техническое решение в сущ. области, относящееся к продукту, устройству, веществу, способу

Объект изобретения ::=

Устройство, вещество, способ, биотехнологический продукт, применение устройства, способа вещества, биотех. продукта по определенному новому назначению.

Новизна ::=

Производство является новым, если оно не известно из уравнения техники (сведения, ставшие общедоступными до даты приоритета изобретения)

Приоритет ::=

Неравенство изобретений, установленное по дате подачи патента

Изобретения, удовлетворяющие критерию изобретательского уравнения, если оно явным образом не следует из уравнения техники

Промышленная применимость ::=

Изобретение может быть использовано на практике в промышленности, здравоохранении и т. д.

Изобретением **не** считаются:

* Открытия, научные теории, математические методы
* Решения, касающиеся только внешнего вида изделий
* Правила и методы
* Программы для ЭВМ
* Предоставление информации

Патент действует 20 лет, с возможностью продления на 5 лет

Полезными моделями не являются:

* Решения, касающиеся только внешнего вида
* Топология интегральных схем
* Решения, противоречащие принципам морали

Промышленный образец ::=

Художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид

Критерии патентоспособности:

* Новизна
* Промышленная применимость
* Оригинальность

Товарный знак ::=

Специальное обозначение для индивидуализации **товаров** юридических и физических лиц.

Знак обслуживания ::=

Специальное обозначение для индивидуализации **услуг** юридических и физических лиц.

Функции товарных знаков:

* Указание правообладателя
* Подтверждение качества
* Получение информации о производителе, продукте и его отдельных свойствах
* Реклама

Единая международная классификация товаров и услуг (МКТУ)