БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сокращения

АРМ – автоматизированное рабочее место
ВИ – видовая информация
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МЭ – межсетевой экран
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ОБПДн – обеспечение безопасности персональных данных
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
РИ – речевая информация
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СПИ – стеганографическое преобразование информации
СЭУПИ – специальные электронные устройства перехвата информации
ТКУИ – технический канал утечки информации
ТСОИ – технические средства обработки информации
УБПДн – угрозы безопасности персональных данных

Общие положения

Модель угроз содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Общие положения

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), связанным:

- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Общие положения

С применением Модели угроз решаются следующие задачи:

- разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;
- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

Классификация угроз безопасности персональных данных

В Модели угроз дано:

- обобщенное описание ИСПДн объектов защиты,
- возможных источников угрозы безопасности персональных данных (УБПДн),
- основных классов уязвимостей ИСПДн,
- возможных видов деструктивных воздействий на ПДн, а также основных способов их реализации.

Классификация угроз безопасности персональных данных

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести:

1. категорию и объем обрабатываемых в ИСПДн персональных данных,
2. структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена,
3. характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн,
4. режимы обработки персональных данных,
5. режимы разграничения прав доступа пользователей ИСПДн,
6. местонахождение и условия размещения технических средств ИСПДн.

Элементы ИСПД

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

- персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;
- информационные технологии, применяемые при обработке ПДн;

Элементы ИСПД

- технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства ИСПДн);

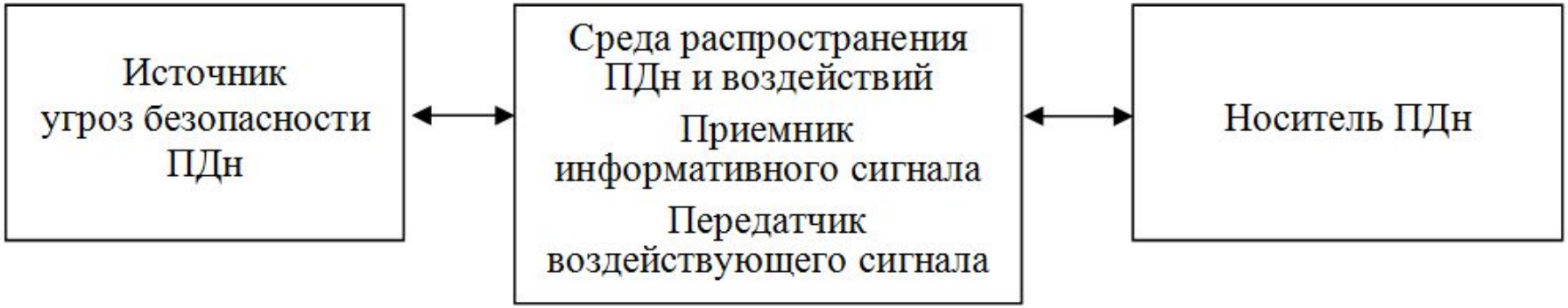
Элементы ИСПД

- программные средства (операционные системы, системы управления базами данных и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в служебных помещениях, в которых расположены ИСПДн (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Источники УБПД

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).



Обобщенная схема канала реализации угроз безопасности персональных данных

Виды информации ПД

Носители ПДн могут содержать информацию, представленную в следующих видах:

- акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;
- видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;
- **информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;**
- **информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.**

Классификация угроз безопасности персональных данных

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками:

- по виду защищаемой от УБПДн информации, содержащей ПДн;
- по видам возможных источников УБПДн;
- по типу ИСПДн, на которые направлена реализация УБПДн;
- по способу реализации УБПДн;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по используемой уязвимости;
- по объекту воздействия.

Классификация угроз безопасности персональных данных

По виду защищаемой от УБПДн информации, содержащей ПДн

- Угрозы РИ
- Угрозы ВИ
- Угрозы информации, обрабатываемой в ТСОИ
- Угрозы информации, обрабатываемой в АС

По видам возможных источников УБПДн

- Создаваемые нарушителем (физическимлицом)
  - Создаваемые внутренним нарушителем
  - Создаваемые внешним нарушителем
- Создаваемые аппаратной закладкой
  - Создаваемые встроенной закладкой
  - Создаваемые автономной закладкой
- Создаваемые вредоносными программами
  - программной закладкой, программой типа "Троянский конь"
  - программным вирусом
  - вредоносной программой, распространяющейся по сети (сетевым червем)
  - другими вредоносными программами, предназначенными для осуществления НСД (подбора паролей удаленного доступа и др.)

По виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн)

- Угрозы конфиденциальности (утечки, перехвата, съема, копирования, хищения, разглашения) информации
- Угрозы целостности (утраты, уничтожения, модификации) информации
- Угрозы доступности (блокирования) информации

По типу ИСПДн, на которые направлена реализация УБПДн

- Угрозы безопасности ПДн, обрабатываемых в ИСПДн на base АРМ (с подключениями и без подключения к вычислительной сети)
- Угрозы безопасности ПДн, обрабатываемых в ИСПДн на base локальной вычислительной сети (с подключением и без подключения к распределенной вычислительной сети)
- Угрозы безопасности ПДн, обрабатываемых в ИСПДн на base распределенных информационных систем (с подключением, без подключения к сети общего пользования)

По способам реализации УБПДн

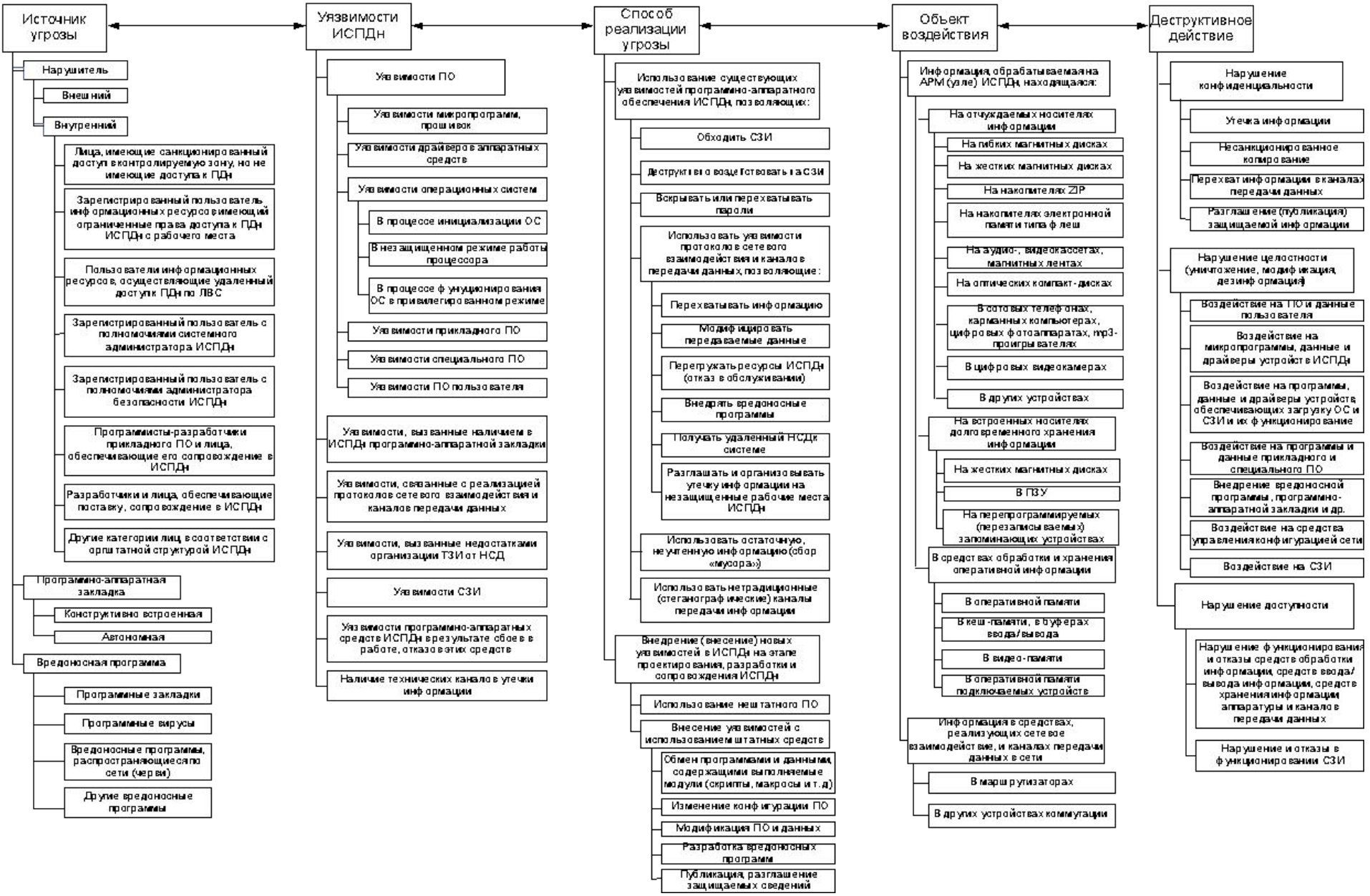
- Угрозы специальных воздействий на ИСПДн
  - механического воздействия
  - химического воздействия
  - акустического воздействия
  - биологического воздействия
  - радиационного воздействия
  - термического воздействия
  - электромагнитного воздействия
    - электрическими импульсами
    - электромагнитными излучениями
    - магнитным полем
- Угрозы НСД в ИСПДн
  - Угрозы, реализуемые с применением программных средств операционной системы
  - Угрозы, реализуемые с применением специально разработанного ПО
  - Угрозы, реализуемые с применением вредоносных програм
- Угрозы утечки информации по техническим каналам
  - по радиоканалу
  - по электрическому каналу
  - по оптическому каналу
  - по акустическому (вибрационному) каналу
  - по смешанным (параметрическим) каналам
  - Угрозы утечки РИ
  - Угрозы утечки ВИ
  - Угрозы утечки информации по каналам ПЭМИН

По используемой уязвимости

- С использованием уязвимости системного ПО
- С использованием уязвимости прикладного ПО
- С использованием уязвимости, вызванной наличием в АС аппаратной закладки
- С использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных
- С использованием уязвимости, вызванной недостатками организации ТЗИ от НСД
- С использованием уязвимостей, обусловливающих наличие технических каналов утечки информации
- С использованием уязвимостей СЗИ

По объекту воздействия

- УБПДн, обрабатываемых на АРМ
  - На отчуждаемых носителях информации
  - На встроенных носителях долговременного хранения информации
  - В средствах обработки и хранения оперативной информации
  - В средствах (портах) ввода (вывода) информации
- УБПДн, обрабатываемых в выделенных технических средствах обработки
  - На принтера, плоттерах, графопостроителях и т.п.
  - На выносных терминалах, мониторах, видеопроекторах
  - В средствах звукоусиления, звуковоспроизведения
- УБПДн, передаваемых по сетям связи
  - УБПДн при передаче сигналов по линиям связи
  - УБПДн при обработке пакетов в коммуникационных элементах информационно-телекоммуникационных систем
- Угрозы прикладным программам, предназначенным для работы с ПДн
- Угрозы системному ПО, обеспечивающему функционирование ИСПДн



Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Общая характеристика уязвимостей информационной системы персональных данных

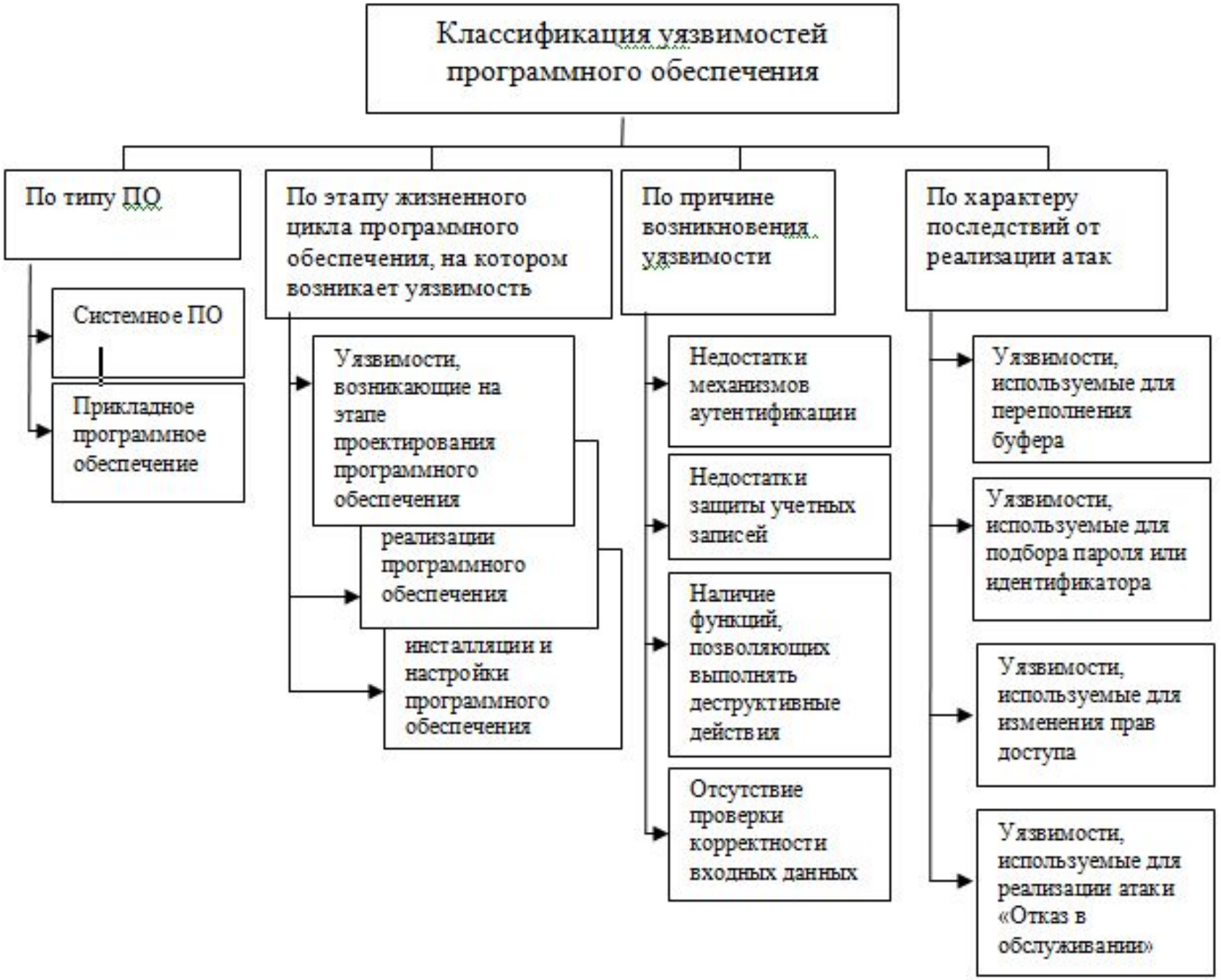
Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

Причины возникновения уязвимостей

- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;


Классификация уязвимостей программного обеспечения
По типу ПО
Системное ПО
Прикладное программное обеспечение
По этапу жизненного цикла программного обеспечения, на котором возникает уязвимость
Уязвимости, возникающие на этапе проектирования программного обеспечения
реализации программного обеспечения
инсталляции и настройки программного обеспечения
По причине возникновения уязвимости
Недостатки механизмов аутентификации
Недостатки защиты учетных записей
Наличие функций, позволяющих выполнять деструктивные действия
Отсутствие проверки корректности входных данных
По характеру последствий от реализации атак
Уязвимости, используемые для переполнения буфера
Уязвимости, используемые для подбора пароля или идентификатора
Уязвимости, используемые для изменения прав доступа
Уязвимости, используемые для реализации атаки «Отказ в обслуживании»