Методы и принципы защиты информации

Терминологическая основа

- **Информацией – сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах.**
- **Информационная безопасность – состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.**

Терминологическая основа

- **<u>Защита информации</u> – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.**

Информационная угроза

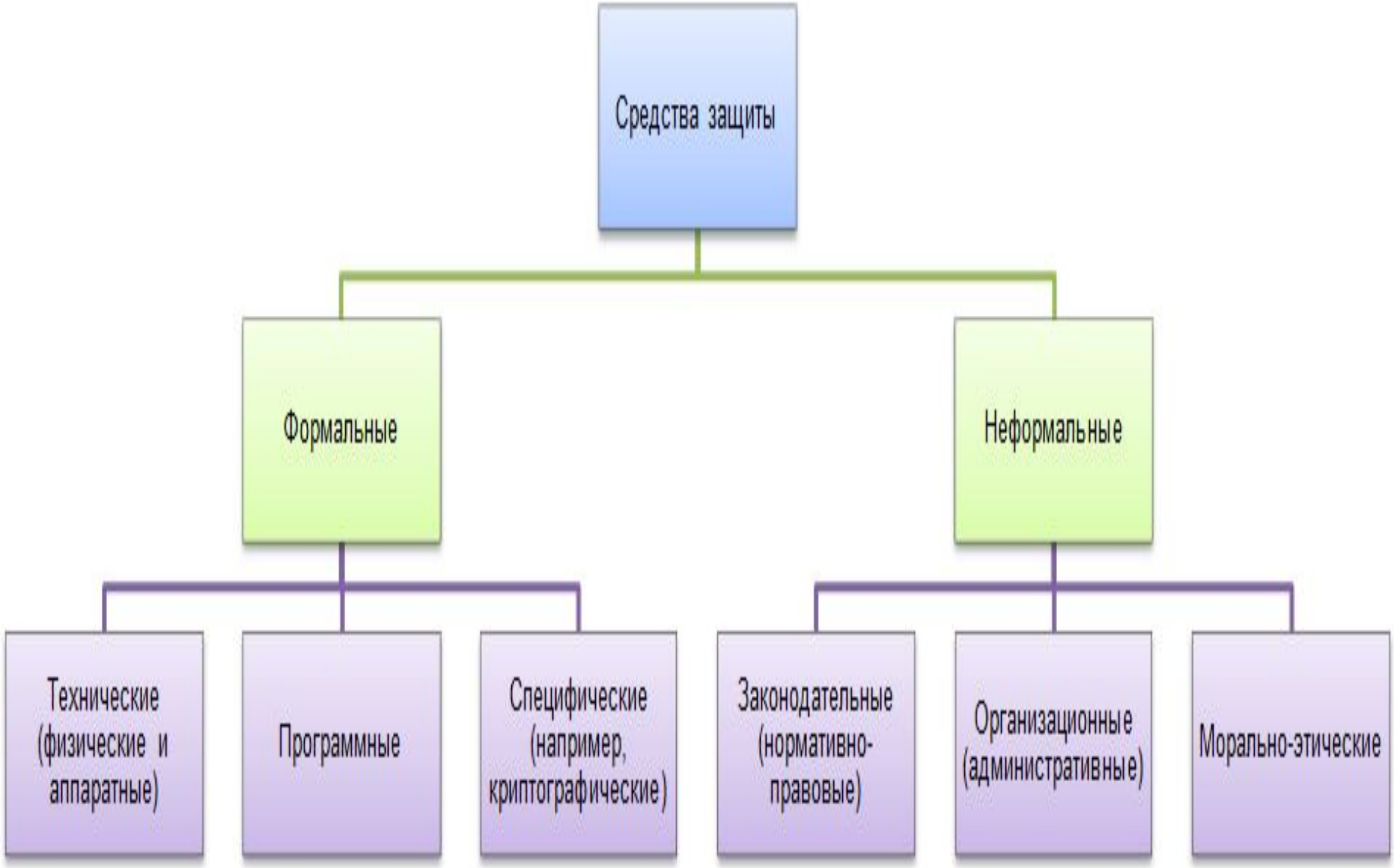
<u>Информационная угроза</u> – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.

Концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:

- Что защищать?
- От чего (кого) защищать?
- Как защищать?

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- **Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;**
- **Целостность – избежание несанкционированной модификации информации;**
- **Доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.**


Средства защиты
Формальные
Неформальные
Технические (физические и аппаратные)
Программные
Специфические (например, криптографические)
Законодательные (нормативно-правовые)
Организационные (административные)
Морально-этические

Средства защиты информации

I. **<u>Формальные средства защиты</u> – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.**

1. <u>Технические средства</u> - защищают информацию от проникновения и утечки:

- **<u>Физические</u> - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).**

Средства защиты информации

- **<u>Аппаратные</u> - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.**

Средства защиты информации

2. <u>Программные средства</u> - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

Средства защиты информации

3. К специфическим средствам защиты информации относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

Средства защиты информации

II. <u>Неформальные средства защиты</u> – регламентируют деятельность человека.

1. <u>Законодательные средства</u> – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений. В настоящее время отношения в сфере информационной безопасности регулируются более чем 80 законами и нормативными документами, иногда достаточно противоречивыми.

- **Международные конвенции об охране информационной собственности, промышленной собственности и авторском праве защиты информации в интернете;**
- **Конституция РФ (принята всенародным голосованием 12.12.1993, вступила в силу 25 декабря 1993, с учетом поправок от 21.07.2014 №11-ФКЗ)**
  - **ст. 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений;**

- **Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018);**
- **Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019):**
  - **ст. 272. Неправомерный доступ к компьютерной информации.**
  - **ст. 273. Создание, использование и распространение. вредоносных компьютерных программ.**
  - **ст. 274 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.**

Средства защиты информации

2. <u>Организационные средства</u> - это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования:

- **Организационно-технические;**
- **Организационно-правовые мероприятия,**

осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем).

Средства защиты информации

3. <u>Морально-этические средства</u> - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета.


Методы защиты информации
Шифрование (криптография) информации
Законодательные меры
Ограничение доступа к информации
Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов
Контроль доступа к аппаратуре
На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения
На уровне защиты компьютерных систем: введение паролей для пользователей
Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры

Методы защиты информации

- **<u>Шифрование</u> - преобразование информации в целях сокрытия от неавторизованных лиц, но в то же время с предоставлением авторизованным пользователям доступа к ней.**
- **<u>Контроль доступа к аппаратуре</u> - внутренний монтаж аппаратуры, технологические органы и пульты управления должны быть закрыты физически и на них установлены соответствующие датчики. При вскрытии аппаратуры оповещающие сигналы должны поступать на центральный пульт сигнализации.**

Методы защиты информации

- **<u>Законодательные (правовые) методы</u> - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. К правовым мерам защиты относятся законы, указы и другие нормативно-правовые акты.**
- **<u>Ограничение доступа к информации:</u>**
  - **На уровне среды обитания человека – выдача документов, установка сигнализации или системы видеонаблюдения.**
  - **На уровне защиты компьютерных систем - введение паролей для пользователей.**

Принципы защиты информации

1. **Комплексность.**
2. **Своевременность.**
3. **Непрерывность**
4. **Активность.**
5. **Законность.**
6. **Обоснованность.**
7. **Специализация.**
8. **Совершенствование.**
9. **Централизация управления.**
10. **Экономическая целесообразность.**
11. **Взаимодействие и координация деятельности.**

Цели защиты информации

1. **Соблюдение конфиденциальности информации ограниченного доступа.**
2. **Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к такой информации.**
3. **Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации.**
4. **Реализация конституционного права граждан на доступ к информации.**
5. **Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.**