# Лекция 1. Определение, понятия область деятельности

## История

Просвещенного профессионализма быть не может без знания (и понимания) истории своей области.

Вопросы защиты информации волнуют человечество давно – всегда было, что скрывать. Вначале это была область интересов **избранных**, а сейчас в данную тему вовлекаются все более **широкие массы**.

Первые документально зафиксированные примеры защиты информации:

- в **Месопотамии** (Двуречье – нижнее течение Тигра и Евфрата – современный **Ирак, Сирия**) глиняные таблички с секретом глазури, 4 век до н.э.

- в средние века переписка знати (**письменность** сама по себе была средством защиты),

- в особо важных документах появляется **шифрование** (Мария Стюарт)

- **переписка военных** в войнах (американцы во второй мировой войне использовали язык индейцев Навахо),

- с 1960-х защита **ресурсов ЭВМ** с военными секретами (носителей, криптография),

В наше время растет **доступность**, поэтому распространилось на **обывателей**:

- **телефон**ные переговоры,

- взаимодействия **офисов** предприятия через сеть Интернет,

- финансовые системы и **электронная коммерция**,

- юридически значимый электронный документооборот (**ЭДО**),

- **защита программ** от нелегального распространения,

- защита от **вирусов** (от программистов).

Периоды развития методов ЗИ:

1. секретная наука для избранных (правители и военные)

- древние времена (сдвиги)

- средние века (многоалфавитность, криптоанализ)

- математическая криптография (перестановки, замены)

2. популяризация (финансовый сектор)

- правило Кергхофа (позапрошлый век)

- открытые дискуссии (персональный компьютеры, бизнес-потребности)

- стандарты и гос.регулирование

- независимость от государств (блокчейн и биткойн)

## Важность вопроса

Обязательство по защите экономической информации (рекомендации, обязательные для исполнения регламентирующие документы и даже принимаются ФЗ о защите информации).

## Определения (из названия курса)

*Из «149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» (последние изменения были внесены 14 июля 2022г. Законом N 374-ФЗ)*

*Добавлены требования к блогерам как к СМИ – более 3 000 в сутки.*

*29 июля 2017 года требование отменено (отмена закона о блогерах)*

**Информация** - сведения (сообщения, данные) независимо от формы их представления (накопленный опыт человечества).

Жизненный цикл информации

Хранение

Выборка

Обработка

Отображение

Конвертация+сохранение

Оценка

Производные данные

Уничтожение

Обновление

Создание

**Документ –** информация,

- зафиксированная на материальном носителе

- снабженная реквизитами.

**Электронный документ** - документированная информация, представленная в электронной форме (воспринимаемой человеком с использованием электронных вычислительных машин, а также передаваемой по информационно-телекоммуникационным сетям)

**Защита информации** - принятие мер

- нормативно-правовых (законы),

- организационно-структурных (внутренние правила организации, направленные на людей),

- технических (программные и аппаратные средства, физическая защита),

направленных на:

1) предотвращение неправомерных действий в отношении информации:

- доступ

- копирование

- модифицирование (изменение)

- блокирование

- предоставление (определенный круг лиц)

- распространение (неопределенный круг лиц)

- уничтожение (удаление)

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Раньше Указом Президента введено «Положение о государственном лицензировании деятельности в области защиты информации» (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. N 10) (последние изменения от 24 июня 1997 г. N 60)

А теперь – Постановление Правительства РФ от 03.02.2012 N 79 "О **лицензировании** деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации") (последние изменения от 15.06.2016)

*------------------------------------------------------------------25 минут-----------------------------------*

*Из «СТО БР ИББС-1.0-2014 от 17 мая 2014 г. «Стандарт Банка России. Обеспечение информационной безопасности организации банковской системы РФ»*

**Актив -**  все, что имеет ценность для субъекта и находится в его распоряжении.

**Информационная сфера:**

* информация,
* информационная инфраструктура (SW, HW, коммуникации),
* субъекты, обрабатывающих информацию,
* процедуры (что делаем),
* система регулирования отношений (что, где, кем, как) – как управлять.

**Угроза –** опасность, предполагающая возможность потерь (ущерба).

**Уязвимость –** свойство системы, допускающее/способствующее реализации угроз

**Безопасность –** состояние защищенности интересов (целей) в условиях угроз.

**Информационная безопасность** – безопасность в условиях угроз в информационной сфере.

|  |  |
| --- | --- |
| Защита информации (процесс) | Безопасность информации (состояние, результат) |

Отличия ЗИ и ИБ

|  |  |
| --- | --- |
| защиты информации | ограничивается информацией |
| информационной безопасности | распространяется на всю информационную сферу |

Информационная безопасность обеспечивает (задачи):

1) доступность (**availability**) – информация предоставляется пользователю в виде и месте, необходимом ему,

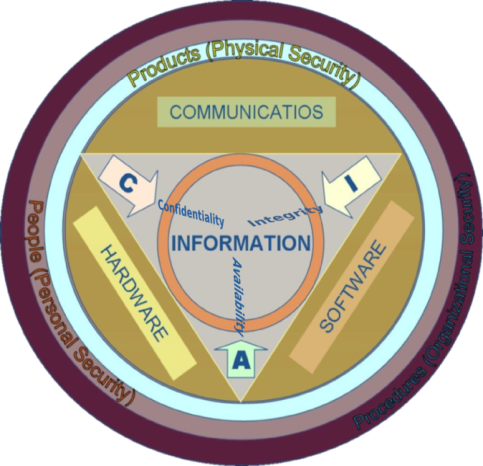
2) целостность (**integrity**) – неизменность информации при передаче и хранении,

3) конфиденциальность (**confidentiality**) – информация предоставляется только авторизованным пользователям.

4) ответственность/неотказуемость – невозможность отказа от авторства.

5) подотчетность – идентификация субъекта доступа и регистрация его действий.

6) аутентичность – подлинность, идентичность заявленному.

****7) достоверность – соответствие предусмотренному поведению или результату.

**Области безопасности**

**Уровни безопасности**

- организационная (процедуры)

- персональная (субъекты)

- физическая (продукты)

Стадии взаимодействия пользователя и системы: регистрация-идентификация-аутентификация-авторизация

**Идентификация** – присвоение и проверка уникального имени объекта (определение пользователя). Пример: логин.

**Аутентификация** – установление и подтверждение подлинности предъявленного пользователем идентификатора (является ли субъект тем, за кого себя выдает).

Пример: двухфакторная аутентификация (фактор владения – ключ, фактор знания – пин-код или пароль).

**Авторизация** – определение и предоставление прав доступа субъекта к защищаемому ресурсу (выполняется компонентом «верификатор»).

## Что охранять и с какими приоритетами

**Приоритеты** при решении задач защиты информации определяются условиями эксплуатации и назначением информационных систем – защищаем то, что определяет **успешность** работы системы **для бизнеса**.

**Ценность актива (информации) –** мера ущерба, наносимого нарушением безопасности актива (информации).

Ценность информации является **критерием** при выборе метода и средств защиты информации.

Важность инфо для бизнеса:

- жизненно важная (без которой невозможно функционирование системы),

- важная (ущерб от потери велик, но может быть восстановлена, или без нее система работает),

- полезная (рабочая информация),

- несущественная.

## Система защиты информации

#### Требования к системе защиты информации

Что учитывать при проектировании:

1. простота

- чем проще, тем прозрачнее->меньше ошибок и неучтенных дыр

- психологическая привлекательность и удобство эксплуатации

2. полнота (учет всех каналов извлечения информации - запуск, выключение, профилактическое обслуживание),

3. ответственность (персональная)

- документально зафиксированное распределение полномочий

- каждый пользователь должен нести ответственность за **каждое** (законное или незаконное) действие

* + - регистрация;
    - идентификация (пользователей, ресурсов и процессов);
    - проверка подлинности (аутентификация);
    - логирование каждого действия

4. обоснованность доступа

- пользователь должен иметь **основания** для доступа к данному виду информации;

- пользователь должен иметь **достаточный** уровень доступа к информации данного вида конфиденциальности;

- полная глубина контроля доступа (должны контролироваться **все** средства доступа ко **всем** ресурсам);

5. разграничение потоков информации

- нельзя помещать секретную информацию на несекретный носитель;

- все ресурсы (внешние устройства, носители, файлы, диски) должны иметь метки с уровнем конфиденциальности (следствие: без метки – не секретный);

6. чистота повторного использования ресурсов

- ресурс (например, оперативная память) должен **гарантированно освобождаться** от предыдущей информации

7. целостность средств защиты

- изолированность от пользователей(прямой доступ должен быть запрещен - информация на носителе должна быть доступна только после выполнения специальных процедур);

- защищенный интерфейс;

- монитор обращений на уровне ОС.

#### Средства защиты информации:

1) Системы аутентификации

* Пароль
* Ключ доступа (физический или электронный)
* Сертификат
* Биометрия
* Одноразовые коды (получаемые через разные каналы)
* Третья доверенная сторона (ЕСИА и др.)

2) Средства авторизации (защиты от несанкционированного доступа)

* различные модели управления доступом;
* журналирование (аудит).

3) Криптографические средства при передаче и хранении

* Шифрование;
* Цифровая подпись.

4) Системы анализа и моделирования информационных потоков

* CASE-системы
* Инструментальные средства анализа систем защиты (до запуска – мониторы, вроде, MaxPatrol)
* Системы мониторинга сетей (после запуска) – поиск нетипичного поведения
  + Системы обнаружения и предотвращения вторжений (IDS/IPS);
  + Системы предотвращения утечек конфиденциальной информации (DLP-системы);
  + Анализаторы протоколов;
  + Pen-тестирование
* Межсетевые экраны.

7) Антивирусные средства и профилактические проверки.

8) Регулярное резервное копирование информации и надлежащее хранение копий.

9) Системы резервирования инфраструктуры

* Источники бесперебойного питания, генераторы;
* Резервирование вычислительных средств и сетевой инфраструктуры;
* Резервирование средств хранения;
* Катастрофоустойчивые системы (географически удаленная копия DataCenter).

10) Режимные меры (ограничение физического доступа к объектам защиты информации)

* Средства предотвращения взлома корпусов и краж оборудования;
* Средства контроля доступа в помещения.

---------------------------------------------------- 45 минут ---------------------------------------------

*Закон 152-ФЗ «О персональных данных» от 27 июня 2006 г. (изменения от 24 апреля 2020)*

Вводит понятия:

- Общедоступные источники ПДн (справочники, адресные книги и т.п.)

- Специальные ПДн (рассовые, религиозные и медицинские данные)

- Биометрические ПДн (позволяют установить личность по физическим особенностям субъекта)

- Трансграничная передача ПДн – требует удостоверения, что принимающая система соответствует правилам защиты соответствующего класса ПДн, установленным Конвенцией. Может быть ограничена «для защиты основ конституционного строя РФ, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства»

Ответственность за нарушение требований 152-ФЗ отражена в кодексах:

- административном

- трудовом

- уголовном

## Методы защиты информации

**Методы (способы) защиты информации –** приемы и операции (действия), реализующие функции защиты.

#### Эволюция средств защиты в электронных средствах

|  |  |  |
| --- | --- | --- |
| **Этап** | **Годы** | **Защитные меры** |
| пока не было персоналок, каждый ходил со своими перфокартами или дискетами (первый дисковод на 8’’ выпустила IBM в 1971 году, для ПК (Apple I) первый дисковод 5,25’’ сделал Стив Возняк в 1978 году) | 1950-1970 | организационные меры |
| при появлении жестких дисков (первый винт – в 1956 году для IBM 305 размером с холодильник и весом в тонну, первый винт, объединивший пластины и головки был сделан IBM, модель 3340 – 1973 год) и их использовании в многопользовательском режиме (тогда же появились и вирусы) | 1970-1990 | идентификация пользователей, пароли |
|  | 1990- | защищенный режим процессора, разделение ресурсов, песочница в SunOS, многопользовательский режим, виртуальные машины |
|  |  | программно-аппаратные средства контроля доступа, ограничивающие доступ к средству, обращающемуся к носителю информации |
|  |  | ортодоксальная изоляция вычислительных средств (либо комплексная защита) |

## Использование пароля для защиты информации

Выбор пароля

1. Простой пароль
   1. Длина ~S^N время для перебора всех возможных комбинаций
   2. Регистрация ошибочных паролей и количества проб для последующего анализ, задержка после неудачного набора
   3. Хищение, подсматривание (не выводить на экран), распечатка и запись (наклеивание на монитор)
   4. Не хранить (и не отображать) пароли в открытом виде (хэш)
   5. Не оставлять пароль в оперативной памяти после использования
2. Модифицированный пароль
   1. Запрашивать отдельные символы пароля (например, 3-й и 5-й)
   2. Однократно используемые пароли (как отрывной блокнот)
3. Вопросно-ответные системы
   1. Стандартные или индивидуальные пользовательские запросы
   2. Усложнить процедуру установления подлинности (пользователь вводит значение функции от предложенного системой значения pass=f(x)
4. Неизменные уникальные характеристики
   1. Отпечатки пальцев
   2. Предоставление доказательств пребывания пользователя в определенном месте в заданное время (поворот ключа)
   3. Подтверждение третьей доверенной стороной/устройством

Методы аутентификации:

- симметричный (претендент и верификатор используют общий секретный ключ, аутентификация в одну сторону)

- несимметричный (одно- и многоразовые пароли, взаимная аутентификация)

#### Меры предосторожности:

- не вырабатывать новый пароль в конце сеанса

- регистрировать факты выполнения процедур «запрос/ответ пароля»

- не оставлять пароли в расшифрованном виде (например, в памяти) после использования.

#### Порядок внедрения средств защиты информации (организационные мероприятия)

1) Проведение аналитического обследования АС

* выявление уровня конфиденциальности информации (что защищать)
* установление уровня полномочий субъектов доступа (кто)
* установление правил разграничения доступа (как)
* создание модели нарушителя

2) Проектирование СЗИ

* выбор методов и средств защиты
* реализация 6 принципов защиты
* документирование (подготовка проектной и эксплуатационной документации).

3) Создание

4) Внедрение и прием СЗИ в эксплуатацию

5) Эксплуатация СЗИ

6) Развитие СЗИ

Жизненный цикл СЗИ описан циклом Деминга:

- планирование (plan)

- реализация (do)

- проверка (check)

- управление / улучшение (act)