История развития систем защиты информации
Лекция 1

Воробьева Алиса Андреевна
Ассистент
Кафедра Безопасных Информационных Технологий,
Университет ИТМО.

Преподаватель

Воробьева Алиса Андреевна

Email: alice_w@mail.ru или через ИСУ

В теме письма: Защита информации + номер группы – **обязательно, иначе письмо потеряется**

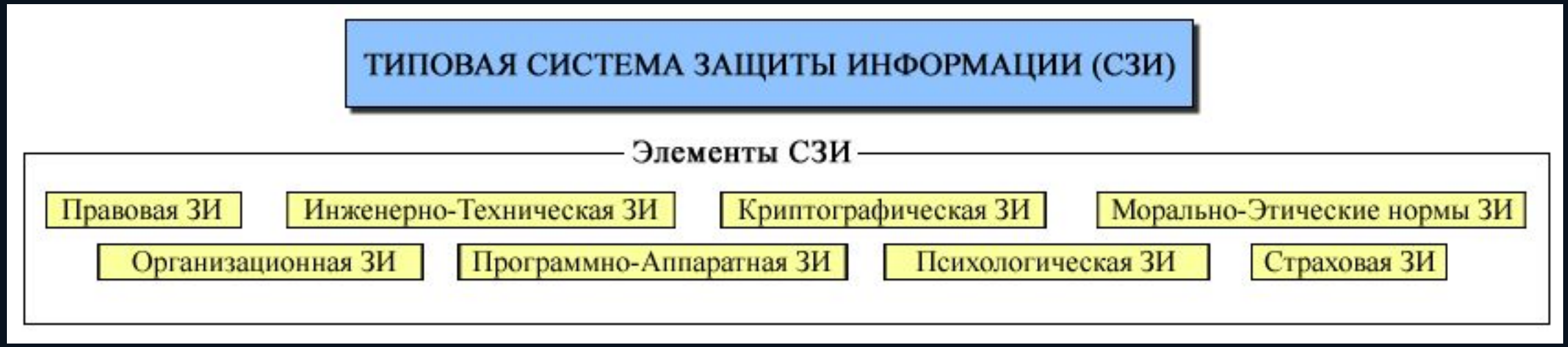
Телефон для экстренной связи: 947-21-14

Защита информации и информационная безопасность

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Современное состояни



Защита информации

- ***Правовая защита информации*** – защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая защита информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является основой для морально – этических норм в области защиты информации.
- ***Организационная защита информации*** – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание *системы защиты,* побуждающих персонал соблюдать правила защиты конфиденциальной информации. Организационные меры связаны с установлением *режима конфиденциальности* в организации.

Защита информации

- ***Техническая*** или ***инженерно-техническая*** защита, основывающаяся на использовании технических устройств, узлов, блоков, элементов, систем, как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации, сооружений и т.д.;
- ***Программно-аппаратная защита***, предполагающая использование программного обеспечения информационных систем, комплексов и систем, а также аппаратных устройств, встроенных в состав технических средств и систем обработки информации.
- ***Математические*** или ***криптографические*** *методы,* которые могут быть реализованы в виде технических устройств, программ и программно-аппаратных средств.

Защиты информации

- ***Психологические*** виды защиты - допускаемые нормами права и морали методы и средства изучения психофизиологических особенностей и возможностей людей, а также психологического воздействия на людей с целью оценки соответствия их требованиям для допуска к обработке защищаемой информации.
- ***Морально-этические*** видами защиты - нормы и правила, которые не имеют юридической силы, но их нарушение ведет к потере авторитета, возникновению дополнительных трудностей и другим негативным последствиям для человека и организации.
- ***Страховая защита информации*** – защита информации, предусматривающая возмещение убытков от её уничтожения или модификации путем получения страховых выплат.

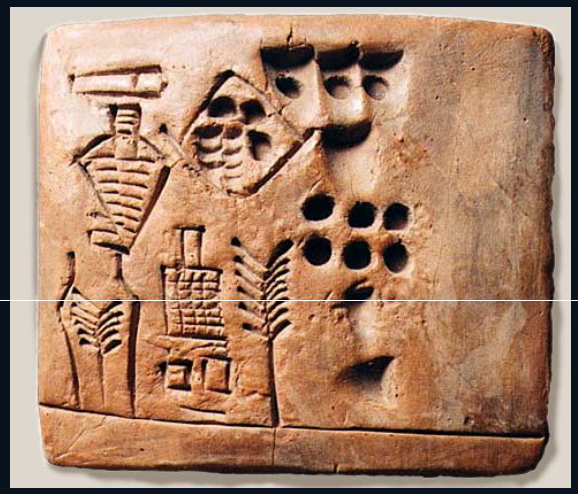
Три базовых принципа ИБ

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного изменения или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Периодизация развития систем ЗИ

I период др. времена - 40-е года XIX в.	Развитие методов шифрования и кодирования, связанное с появлением письменности
1 этап: др. времена – конец XV в.	Наивная криптография: стеганография, кодирование, моноалфавитные шифры, тайнопись.
2 этап: конец XV – 40х гг. XIX вв.	Формальная криптография: появление формализованных и относительно стойких к ручному криптоанализу шифров, шифры многоалфавитной замены, роторные криптосистемы
II период 50-е года XIX века - 50-е года XX в.	Развитие методов защиты информации по техническим каналам, связанное с появлением телефона, телеграфа, радио
III период 50-е года XX века – до наших дней	Становление проблемы информационной безопасности, связанное с появлением ЭВМ. Развитие методов компьютерной безопасности. Научная криптография (1930 – 60-е гг.) и компьютерная криптография.

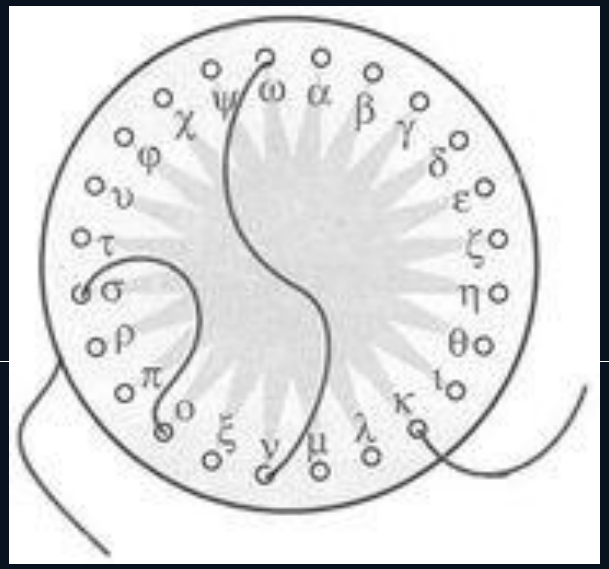
I период (др. времена - 40-е года XIX века)

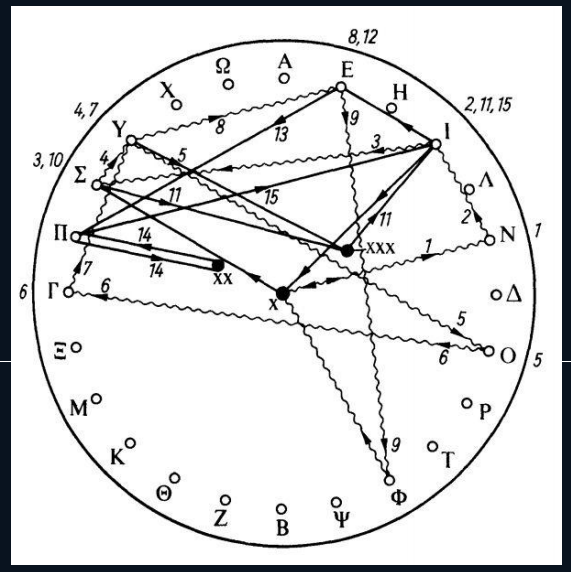


Глиняные таблички, др. Месопотамия

Скитала, шифр древней Спарты

I период (др. времена - 40-е года XIX века)





Диск Энея (Др. Греция, IV век до н. э.)

	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Y
5	Φ	X	Ψ	Ω	

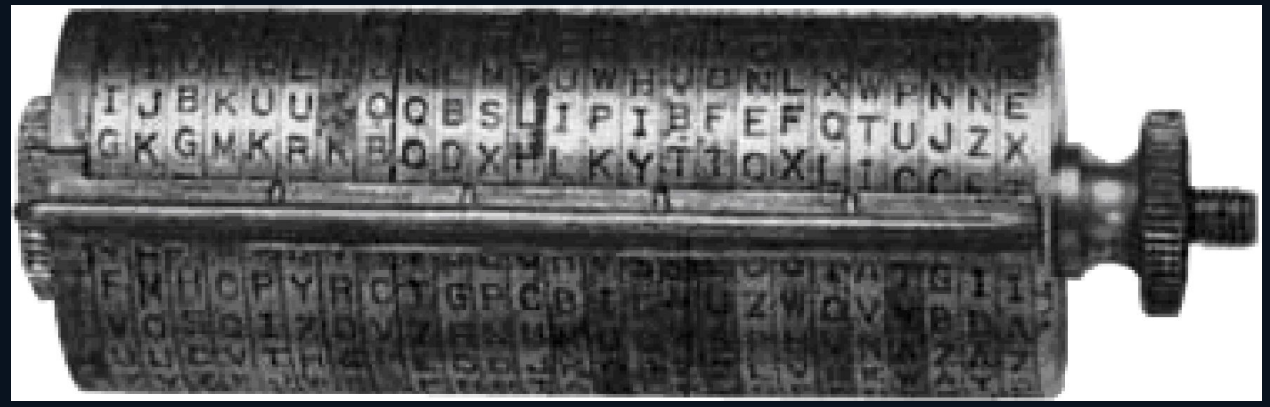
Квадрат Полибия (Др. Греция, II век до н. э.)

I период (др. времена - 40-е года XIX века)

- Первые работы по криптографии и криптоанализу
  - 1466 г. - Леон Батисте Альберти, «Трактат о шифре» - первая научной работа по криптологии.
  - 1508 г. - аббат Иоганн Трисемус, «Полиграфия»
  - 1883 г. – Огюст Керкхофф, «Военная криптография»
- Роторные криптосистемы

(Шифратор Джефферсона.

Начало XIX века)



Периодизация развития систем ЗИ

Период	Описание
I период др. времена - 40-е года XIX в.	Развитие методов шифрования и кодирования, связанное с появлением письменности
1 этап: др. времена – конец XV в.	Наивная криптография
2 этап: конец XV – 40х гг. XIX вв.	Формальная криптография
II период 50-е года XIX века - 50-е года XX в.	Развитие методов защиты информации по техническим каналам, связанное с появлением телефона, телеграфа, радио
III период 50-е года XX века – до наших дней	Становление проблемы информационной безопасности, связанное с появлением ЭВМ. Развитие методов компьютерной безопасности. Научная криптография (1930 – 60-е гг.) и компьютерная криптография

II период (50-е года XIX века - 50-е года XX века)

- Шифрование и разграничение доступа по принципу доверенных лиц.
- Развитие методов защиты информации от утечек по техническим каналам, связанное с появлением телефон, телеграф, радио.
- работы Алана Тьюринга и машина «Энигма»

III период (50-е года XX века – до наших дней) Развитие ЗИ и компьютерной безопасности

- 1 этап: 1950-вторая половина 1970-х. Мейнфреймы, фрикеры и первые хакеры
- 2 этап: вторая половина 1970-х - начало 1990-х годов. Персональные компьютеры и сети
- 3 этап: 1994- 2000 World Wide Web и Microsoft. Расцвет компьютерных преступлений
- 4 этап: 2001 - настоящее время. Кибербезопаность. Кибертерроризм, социальные сети и Интернет-вещей

1 этап: 1950-вторая половина 1970-х

1. Появление и распространение первых ЭВМ.
2. Появление первых хакеров: лучших компьютерных специалистов.
3. Появление первых компьютерных преступлений: ЭВМ или компьютерная система – цель атаки.
4. Большое число телефонных фрикеров.
5. Основные угрозы: утечки по техническим каналам, угрозы сбоев в электропитании и угрозы электронного перехвата
6. Появление первых систем и стандартов компьютерной защиты информации.
7. Появление компьютерной криптографии.
8. Появление систем разграничения доступа в компьютерных системах, основанных на парольной идентификации.
9. Развитие систем контроля управления доступом.

1 этап: 1950-вторая половина 1970-х

- ***Компьютерные преступления*** - физическое воздействие с целью вывода из строя или нелегальное использование компьютерных систем и телефонных линий, компьютерный саботаж.
- ***Хакер*** – специалист, исключительно положительное значение, отражающее высокую квалификацию.
- ***Хак*** - элегантное и эффективное программное решение, требующее меньшего количества машинных команд и с более эффективным управление оперативной памятью.

1 этап. **Уязвимости, ARPANET и первые компьютерные вирусы**

1965 – первые сообщения о уязвимостях
1969 - ARPANET
1972 – email (Рэй Томлинсон)
Начало 1970-х - первые компьютерные вирусы (Creeper, Rabbit, Pervading Animal)

1 этап. Виды компьютерных преступлений

Атаки, устоявшийся от внутренних источинков => Меры защиты

Только от внутренних угроз и внешнего физического воздействия

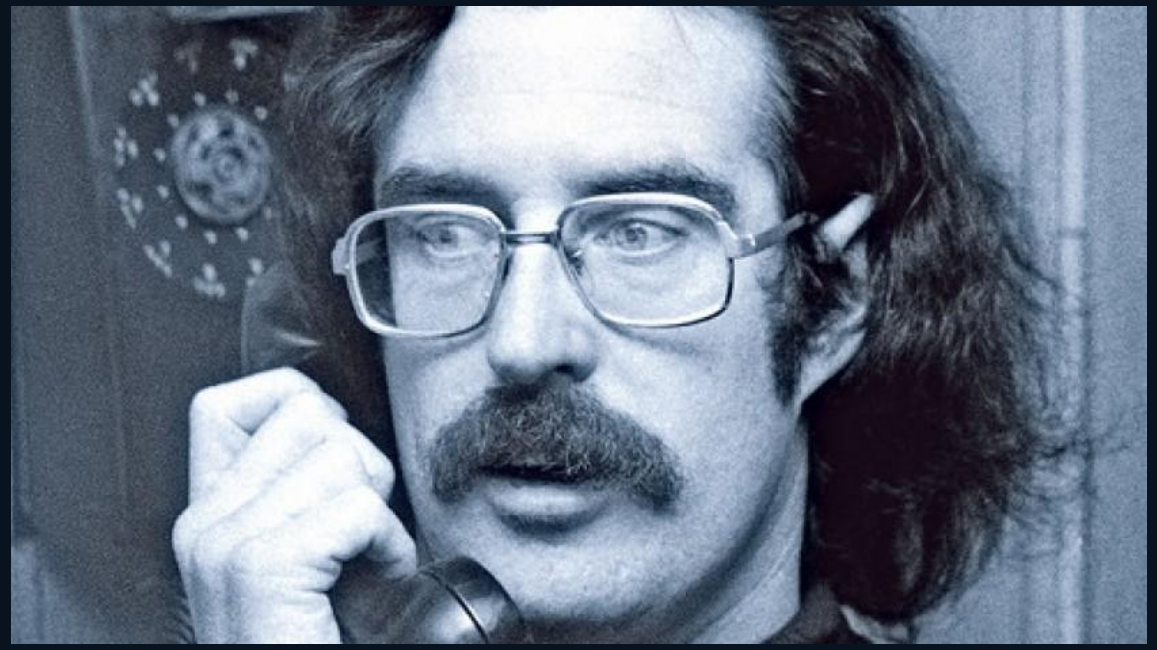
Компьютерный саботаж - физическое воздействие на компьютеры с целью их порчи, отключения или уничтожения.

Подделка компьютерных данных - незаконное или несанкционированное изменение (модификация) информации. Модификация может производиться на всех этапах работы: при вводе или выводе данных, их обработке.

Кража компьютерной информации и вымогательство

1 этап. **Телефонные фрикеры**

- 1957 – Джои Энгрессиа. В 1968 году задержан ФБР
- 1971 - Джон Дрэйпер («Капитан Кранч»)
- «Multi Frequency box» или «blue box»



1 этап. **Защита информации**

Разработки и исследования для военных и правительственных организаций

1950-е Основные задачи:

1. Физическая и организационная защита объектов компьютерной инфраструктуры от кражи, порчи, саботажа и угроз природного характера.
2. Контрольно-пропускной режим, различные типы сигнализаций.
3. Физическая безопасность носителей информации и защта от сбоев в электропитании.

1960-1970-е Основные задачи:

1. Безопасность данных, содержащихся в хранилищах и базах данных.
2. Безопасность операционных систем.

1 этап. **Защита информации. Военные и правительственные организации**

- ***Парольные системы идентификации***
- ***Стандарты компьютерной безопасности***

1. Стандарты исследования, проектирования, создания, тестирования и эксплуатации безопасных компьютерных систем;
2. Государственные криптографические стандарты.

1970 – отчет научного совета обороны в рамках МО США, содержащий базовые принципы обеспечения безопасности конфиденциальной информации:

решение задач защиты на этапе проектирования системы,

принципы открытой и закрытой среды, конфиденциальная информация должна обрабатываться только в закрытой среде.

1 этап. **Защита информации. Военные и правительственные организации**

- ***Криптография*** - аутентификация, верификация и безопасности военной и правительственной коммуникации.

1 этап. **Защита информации. Военные и правительственные организации**

- **Мандатное управление доступом (англ. Mandatory access control, MAC)** — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

- **Дискреционное упревление доступом(избирательное управление доступом, англ. discretionary access control, DAC)** — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

1 этап. **Защита информации. Военные и правительственные организации**

- ***Модели разграничения доступа***
  - Концепция «ядра безопасности» МО США
- модель Белла-ЛаПадула
- модель Биба
- Формальные модели
  - дискреционная модель Харрисона-Руззо-Ульмана
  - модель Take Grant
  - модель безопасности информационных потоков

1 этап. **Защита информации. Военные и правительственные организации**

- ***Системы контроля управления доступом***
  - Пароли
  - Магнитные карты
  - бесконтактные карты (proximity карты)
  - RFID метки

2 этап: вторая половина 1970-х - начало 1990-х годов. Персональные компьютеры и сети.

- Появление первых ПК
- Появление единого сетевого протокола TCP/IP
- Появление Bulletin Board Systems (BBS)
- Трансформация ARPANET в Internet

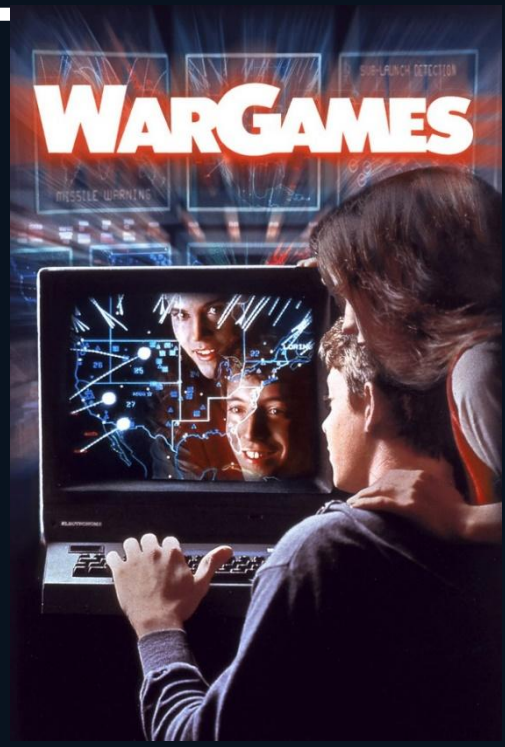
- Появление коммерческих компьютерных и сетевых сервисов

2 этап. Компьютерные преступления

- Трансформация образа хакера. Негативный оттенок.
- Взлом и НСД к компьютерным системам
- 1970-е: хакеры – «одиночки»
- 1980-е: первые хакерские группы и объединения, хакерские журналы и конференции

- Взломы и НСД к компьютерным системам
- Компьютерные вирусы и эпидемии
- Компьютерный шпионаж

2 этап. Компьютерные преступл



- «Военные игры» (1983)
- Группа хакеров 414
- первые хакерские объединения (Legion of Doom, Masters of Desception и Chaos Computer Club)

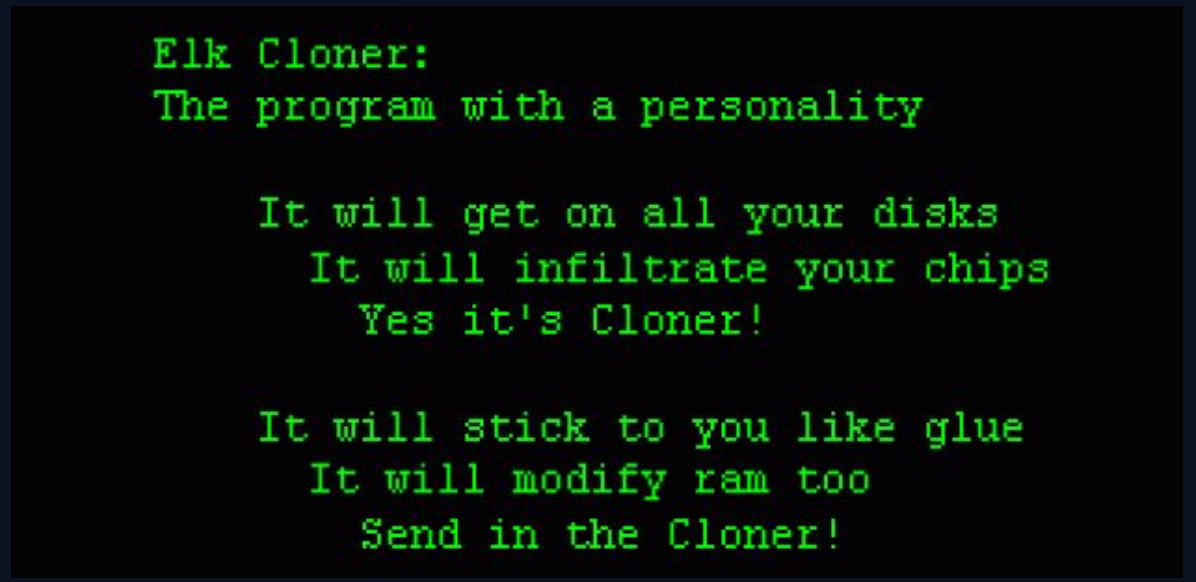
Первые законы о компьютерных преступлениях

- **1984 -** Data Protection Act (Великобритания)
- **1986 –** Computer Fraud and Abuse Act и Electronic Communication Privacy (США)

2 этап. Компьютерные преступления. Вирусы

- Вирусные эпидемии (Elk cloner, Brain, Vienna)
- 1988 – Червь Морриса
- Сетевые черви (Father Christmas, WANK, Lehigh, Stoned, Jerusalem, Cascade, DATACRIME, Ping-Pong, Form, Michelangelo)

- Появление:
  - файловые и загрузочные вирусы;
  - вирусы-компаньоны.
  - стелс-вирусы
  - сетевые вирусы, черви;
  - полиморфные вирусы;
  - многокомпонентные вирусы.



2 этап. Защита информации. Коммерческие организации, персональные компьютеры и сети

- Компьютерная безопасность - обеспечение конфиденциальности данных и доступности компьютерных ресурсов, защиту процессов от неправомерного использования или несанкционированных изменений.

2 этап. Защита информации. Коммерческие организации, персональные компьютеры и сети

- Модели разграничения доступа для коммерческих организаций
- Появление биометрических систем идентификации и аутентификации
- Появление межсетевых экранов
- Развитие криптографии:
  - правительственной – стандарт DES
  - «общественной»: работы Диффи-Хеллмана и алгоритм RSA
- Появление антивирусного ПО
- Новые государственные и международные стандарты компьютерной безопасности
- Появление групп CERT (Computer Emergency Response Team)

2 этап. Защита информации. Угрозы

Появление новых угроз:

- вызванных, уязвимостями различных сетевых протоколов (в частности, TCP/IP) и систем;
- атаки вирусов и сетевых червей;
- опасность осуществления НСД к данным или ресурсам компьютерной системы;
- несанкционированный перехват данных и их модификация;
- кража паролей.

Источники угроз и инициаторы атак - хакеры, конкурирующие организации, инсайдеры (в том числе недовольные сотрудники).

2 этап. Разграничение доступа и межсетевые экраны

Разграничение доступа

- Модели разграничения доступа для коммерческих организаций
  - модель Кларка-Вильсона
  - модель Китайская стена
  - модель Гогена-Мезигера
- Биометрические системы разграничения доступа
  - Цель: идентификация личности, СКУД, контроль рабочего времени.

Межсетевые экраны

1. 1988 - Фильтрующие маршрутизаторы
2. 1989 - Шлюзы сеансового уровня

2 этап. Криптография, антивирусы и «Оранжевая книга»

Криптография

1. Компьютерные блочные шифры: стандарт DES
2. Появление ассиметричных шифров и систем с открытым ключом: алгоритм Диффи-Хеллмана и алгоритм RSA

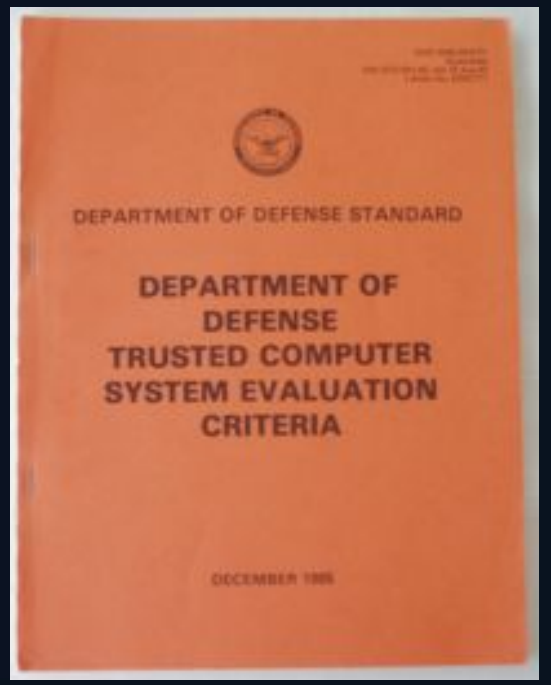
Антивирусные технологии

1. Синтаксический анализ
2. Появление первых вирусных баз
3. Эвристический анализ
4. Сигнатурный анализ

Крупные антивирусные компании:

1. McAfee и Symantec

1983 – **Trusted Computer System Evaluation Criteria** (Оранжевая книга)



Лекция 2

3 этап: 1994- 2000 World Wide Web и Microsoft

1991 – первые веб-страницы
1994 – первый браузер Netscape Navigator

Хакерское ПО в массы: winnuke, Netbus и BackOrificeБ, ss
Хакерство – массовое явление

1995 – Windows 95
1998 – DoS-атаки МО США
1999 – год уязвимостей продуктов Microsoft

MICROSOFT®
WINDOWS™ 95

Microsoft® Internet Explorer 5

3 этап: 1994-2000 Компьютерные преступления

1. Компьютерные вирусы

- Массовые вирусные эпидемии компьютеров под ОС Microsoft
- Макровирусы
- Почтовые вирусы

2. Компьютерные взломы

- Владимир Левин и CitiBank
- Взлом МО США

3. Социальная инженерия в компьютерных преступлениях

- Кевин Митник

3 этап: 1994-2000 Компьютерные преступления

4. Компьютерное мошенничество и угрозы электронной коммерции

- Мошенничество с кредитными картами
- **Спам (**Лоуренс Кантер и Марта Сигел**)**

5. Отказ в обслуживании DoS и DDoS атаки (почтовые бомбы, первые флуд-атаки)

  - Первые инструменты для DDos атак (Fapi, Trinoo, TFN (Tribal Flood Network), Stacheldraht, Mstream, Omega, Trinity, Derivatives, myServer, Plague)
  - MafiaBoy (против eBay, CNN, Yahoo и Amazon)

6. Кибертерроризм и хактивизм

7. Компьютерная порнография

3 этап: 1994-2000 Защита информации

Криптография и криптографические стандарты

- S/MIME (Secure Multipurpose Internet Mail Extensions)
- SSL
- S-HTTP и HTTPS
- **AES: новый стандарт МО США**

Развитие программных средств защиты информации

- Антивирусное ПО
- Межсетевые экраны: шлюзы прикладного уровня
- Системы обнаружения вторжений (IDS)
    - 1. Сетевые IDS (1984-1993 - Экспертные системы: IDES, NIDES)
    - 2. Узловые IDS: SNORT

3 этап: 1994-2000 Защита информации

Системы разграничения доступа

- Модели разграничения доступа
  - 1992 - Дэвид Феррайоло и Ричард Кун - Ролевое разграничение доступа (Role-based access control, RBAC)
  - Модель Санди, Феррайоло и Куна – единый стандарт RBAC
- Биометрические системы разграничения доступа
- Программно-аппаратные системы разграничения доступа
  - RSA SecurID

3 этап: 1994-2000 Защита информации

Новые стандарты компьютерной безопасности

- 1990 - Information Technology Security Evaluation Criteria (Европа)
- 1993 - Canadian Trusted Computer Product Evaluation Criteria (Канада)
- 1996 – первый международный стандарт - Common Criteria, ISO 15408 (Общие критерии)
- 1996 – COBIT (управление и аудит)

Итоги

История защиты компьютерной информации:

1. По запросу военных и правительства – меры защиты и контроль военных и спецслужб.
2. По запросу коммерческих организаций и пользователей – меры защиты совместно ИТ-компаниями и научными организациями. Контроль – службы безопасности, спецслужбы и органы полиции.

Этапа развития средств защиты:

1. Нет сетей – физическая и организационная защита.
2. Сети – защита извне, защита на периметре – средства сетевой защиты.
3. Инсайдеры – защита от внутренних угроз – средства обнаружения утечек.
4. Развитие систем прогнозирования и предотвращения атак.