Кафедра № 12
Компьютерные системы и технологии

Защищенные компьютерные технологии: миф или реальность?

Иванов М.А.

Москва, 2025

Иванов Михаил Александрович

maivanov@mephi.ru
https://discord.gg/TW6TaSj

Канал «Защита информации»

Темы

1) Причины трудоемкости решения задач ЗИ
2) Стохастические методы ЗИ. Особенности криптографии как науки
3) Основы криптологии. Основные термины и определения. Классификация шифров. Требования к качественному шифру
4) Криптосистемы с секретным ключом. Обоснование стойкости. Блочные и поточные шифры. Принципы и примеры их построения. Криптоалгоритмы ГОСТ 29147-89*, AES-128, Кузнечик, RC4*. Неоднородное ключевое пространство
5) Криптосистемы с открытым ключом. Обоснование стойкости. Принципы и примеры их построения. Криптосистема RSA. Криптосистема Меркля-Хеллмана. Криптографические бэкдоры
6) Примитивные и прикладные криптографические протоколы. Протоколы выработки общего секретного ключа, электронной подписи, аутентификации удаленных абонентов, разделения секрета, доказательства с нулевым разглашением знаний. Схема Kerberos

Темы

8) ЗИ в электронных платежных системах (ЭПС) на основе цифровых денег
9) Биткоин. Блокчейн
10) Программные средства скрытого информационного воздействия (РПВ, разрушающие программные воздействия)
11) Методы антивирусной защиты. Структура и состав комплекса программных средств антивирусной защиты (КПС АВЗ)
12) Функции генераторов псевдослучайных чисел (ГПСЧ) в системах ЗИ*. Требования к качественному ГПСЧ, требования к качественной хеш-функции (ХФ)*
13) Идентификация, аутентификация и авторизация. Парольные системы разграничения доступа*
14) Управление ключами*
15) Причины ненадежности криптосистем*
16) Алгоритмическое мышление в задачах ЗИ*

Источники информации

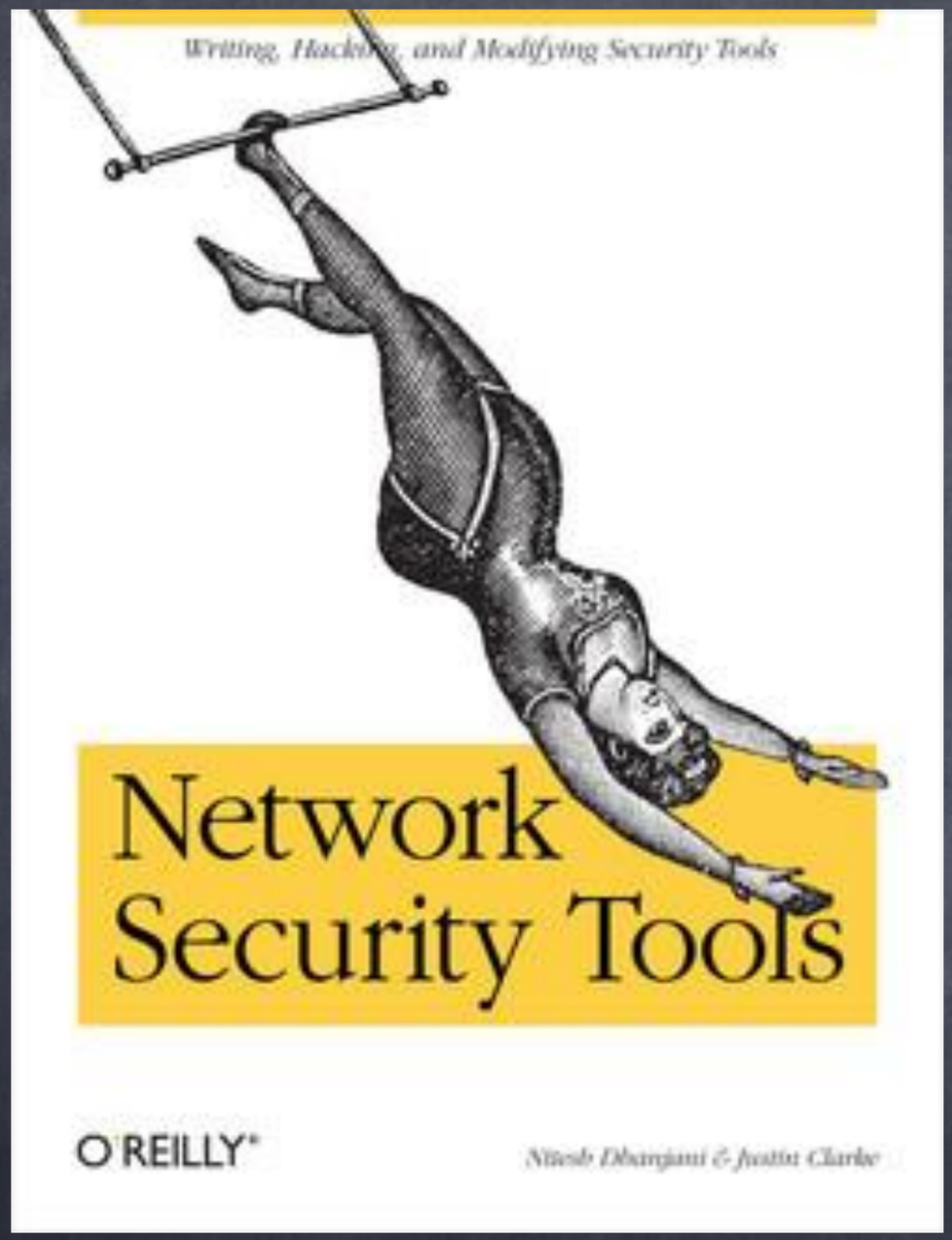
1) Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, «ЧеРо», 1998.
2) Брассар Ж. Современная криптология: Пер. с англ. – М.: ПОЛИМЕД, 1999.
3) Мао В. Современная криптография: теория и практика: Пер. с англ. – М.: Издательский дом «Вильямс», 2005.
4) Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. - М.: Горячая линия-Телеком, 2005.
5) Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. – М.: Издательский дом «Вильямс», 2005.
6) http://www.enlight.ru/ (А. Винокуров)

---

7) Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: НИЯУ МИФИ, 2012.
8) Иванов М.А., Саликов Е.А. Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. – М.: НИЯУ МИФИ, 2021.
9) Иванов М.А. Основы криптографии. В 2-х частях. – М.: ГУУ, 2023.
10) Иванов М.А. Безопасность искусственных когнитивных систем. Методы поиска новых технических решений. – М.: НИЯУ МИФИ, 2025.

Источники информации на английском языке

1) Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. 2nd Edition, CRC Press, 2015.
2) William Stallings. Cryptography and network security. Principles and practice. Sixth Edition. Prentice Hall, 2014.
3) Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography. 2015. crypto.stanford.edu/~dabo/cryptobook/
4) Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.
5) Niels Ferguson and Bruce Schneier. Practical Cryptography. Wiley Publishing, 2003.
6) Goldwasser-Bellare lecture notes. http://www.cs.ucsd.edu/users/mihir/papers/gb.pdf
7) Barak's lecture notes. http://www.cs.princeton.edu/courses/archive/fall05/cos433
8) Eric Filiol. Computer viruses: from theory to applications. Springer-Verlag, 2005.
9) Jon Erickson. Hacking: the art of exploitation. 2nd Edition. No Starch Press, 2008.
10) Adam Young, Moti Yung. Malicious Cryptography: Exposing Cryptovirology. 2004.



Network Security Tools
Nitesh Dhanjani,
Justin Clarke
O'REILLY, 2005

Машинное обучение и безопасность. Серия O'REILLY ДМК Пресс, 2020
Кларенс Чио
Дэвид Фримэн

Задания для самостоятельной работы

1) Основная задача: рассказать просто о сложном
2) Рисунки и схемы алгоритмов приветствуются (код нужен в последнюю очередь)
3) За хороший отчет зачет или экзаменационную оценку ставлю сразу
4) Остальные отчеты придется защищать на зачете или экзамене
5) Желающие могут выступить

Форматы файлов только .PDF и .RTF !!!

Темы заданий для самостоятельной работы

1) Атака Нострадамуса
2) Уязвимости аппаратного обеспечения (процессоров)
   и описание принципов их использования
3) Физически неклонируемые функции (PUF).
   Не менее двух схем. Временные диаграммы приветствуются
4) SETUP-атаки. Не менее трех примеров
5) LDPC-коды. Базовая идея. Пример построения кодера и декодера*
6) Полярные коды. Базовая идея. Пример построения кодера и декодера*
7) Модификации поточного шифра RC4 (RC4+). Схемы алгоритмов. ~~Spritz~~
8) Описание собственного бэкдора для криптосистемы
   с открытым ключом (RSA, Knapsack, El Gamal, Shor-Rivest) + пример
9) Криптографические бэкдоры в блокчейне
10) Новые конструкции хеширования ChopMD, 3C, 3C+ и др.
    (не менее трех - схемы, базовые идеи). ~~Sponge~~ *
11) Бэкдоры и технологии ИИ*
12) Модификации технологии OAEP (OAEP+). Схемы и базовые идеи.
    Не менее трех

Темы заданий для самостоятельной работы

1) Программная реализация шифра Ф. Бэкона (2)
2) Программная реализация модифицированного шифра Ф. Бэкона (4)
3) Программная реализация бэкдора для криптосистемы RSA (2)
4) Программная реализация бэкдора для ранцевой криптосистемы (2)
5) Программная реализация бэкдора в ГПСЧ*
6) Программная реализация дихотомических ГПСЧ И.А. Кулакова
7) Программная реализация ГПСЧ RC4 (два режима)
8) Программная реализация модифицированного ГПСЧ RC4 (4) (два режима)
9) Программная реализация ГПСЧ Spritz* (два режима)
10) Программная реализация ГПСЧ С.А. Осмоловского (два режима)

1) - 5) д.б. два режима работы – демонстрационный и учебный
6) - 10) д.б. возможность изменять исходные параметры, в том числе длину ПСП, которую ВЖИВУЮ надо писать в файл

Защищенные компьютерные технологии: миф или реальность?

Проблема кибербезопасности

Информационно-психологическая война

Информационно-техническая война

Политика коммерческих компаний

Уязвимые IT-технологии

Сложность информационных систем

Все большее отстранение пользователей от реальных процессов обработки информации

Человеческий фактор

Существует еще одна причина
- повсеместное использование
криптографии

Информационная война

Информационно-психологическая война

Информационно-техническая война

Кибервойна
(война в киберпространстве)

Оборонительное кибероружие

Наступательное кибероружие

Информационно-психологическая война уже давно идет !

- Манипуляция сознанием
- Психология влияния
- Нейролингвистическое программирование
- Социальная инженерия
- Обратная социальная инженерия
- Технология обмана

Кибервойна уже давно идет !

Только две истории

- Stuxnet
- Рейтинг США

Веритофобия
- ужас правды,
неумение видеть правду,
нежелание знать ее

Internet

- Worms and Trojans
- DDoS-attacks, Botnets
- Exploiting Zero Days Vulnerabilities

Internet of Things

- Worms and Trojans
- Botnets of Smart Things
- Exploiting Zero Days Vulnerabilities of Smart Things

Internet of Values

- Worms and Trojans
- DDoS-attacks, Mining Botnets
- Exploiting Zero Days Vulnerabilities

Internet of Everything

- ???

К концу 2020 года к Интернету было подключено более 200 миллиардов устройств

Актуальные угрозы кибербезопасности

Exploiting Software Vulnerabilities

Phishing

Ransomware

Cryptojacking

APT Attacks

Exploiting Hardware Vulnerabilities

Все IT-технологии уязвимы !

Supercomputer

Mobile

RFID

Cyber-Physical

Появление и развитие суперкомпьютерных технологий

Стало намного проще решать задачи полного или частично-полного перебора

→ взлом криптоалгоритмов и криптопротоколов

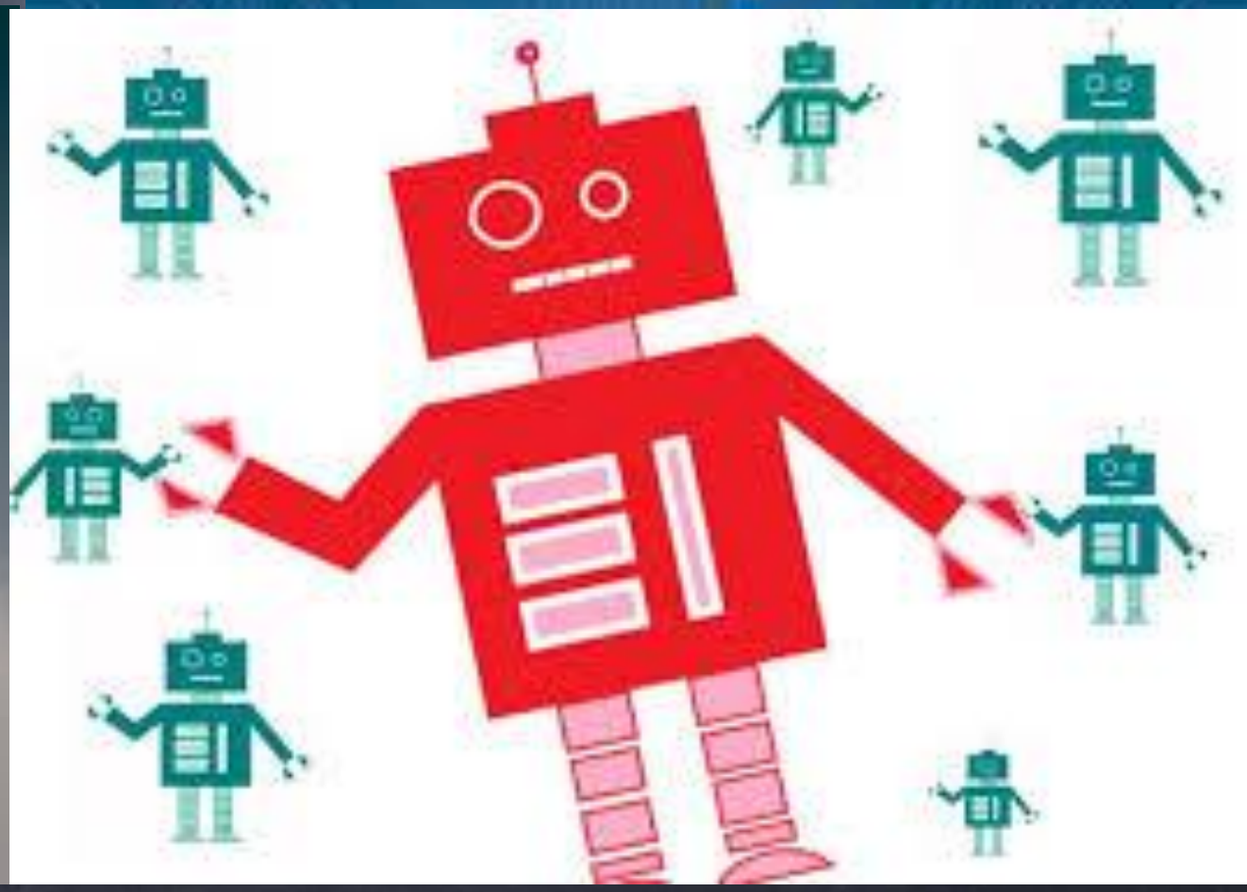
→ поиск уязвимостей ПО → участились случаи обнаружения разрушающих программных воздействий (РПВ), использующих уязвимости нулевого дня (**Zero Day Vulnerabilities**)

→ существенное снижение требований к пропускной способности скрытых каналов утечки информации → появились РПВ, использующие скрытые каналы

Основные угрозы безопасности киберфизических систем (КФС) (Cyber-Physical Systems)

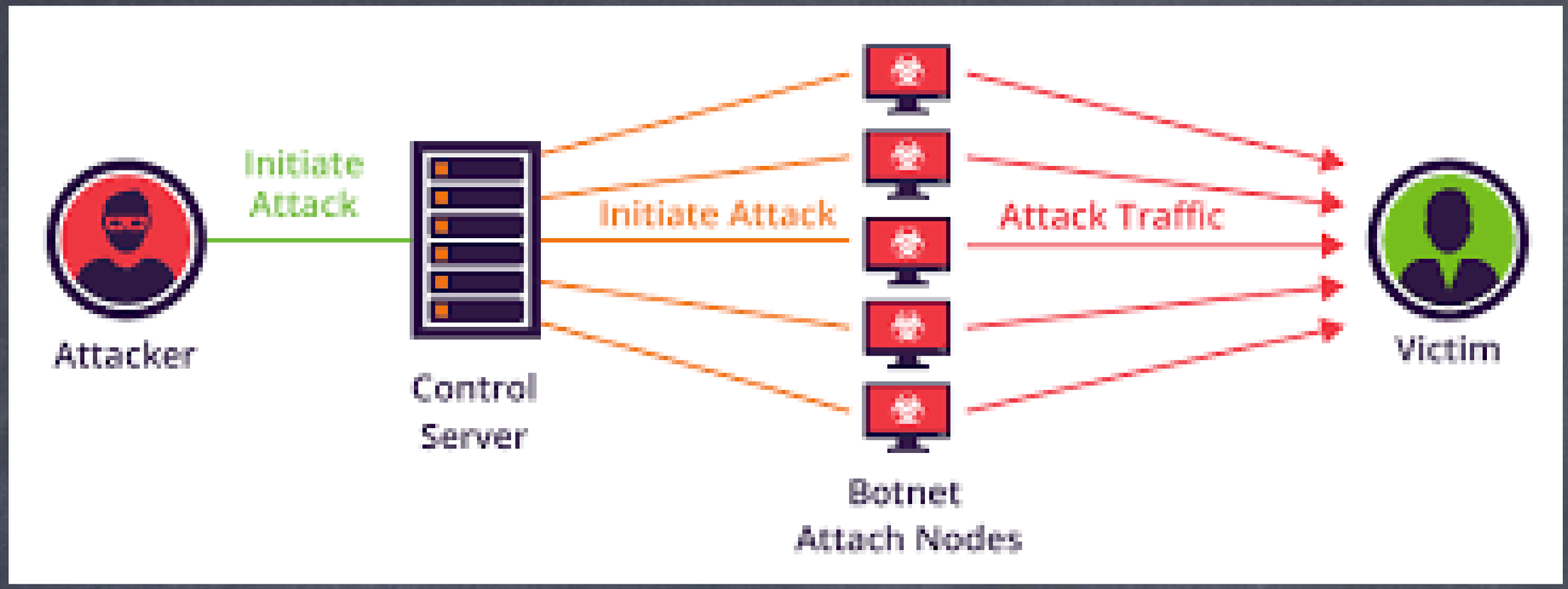
- Разрушение систем управления. Результат – потеря контроля над КФС
- Подмена алгоритма функционирования
- Воздействие на поведение человека посредством искажения информации, получаемой им от КФС
- Подмена сигналов GPS/Глонасс мобильной КФС → полная потеря работоспособности, поскольку изменены координаты КФС (мобильного робота)
- Воздействие на оператора КФС. Человек (оператор КФС) – слабое звено! Необходим постоянный мониторинг психо-физического состояния человека-оператора

«Умная» кукла с ИИ способна распознавать эмоции ребенка и реагировать на них

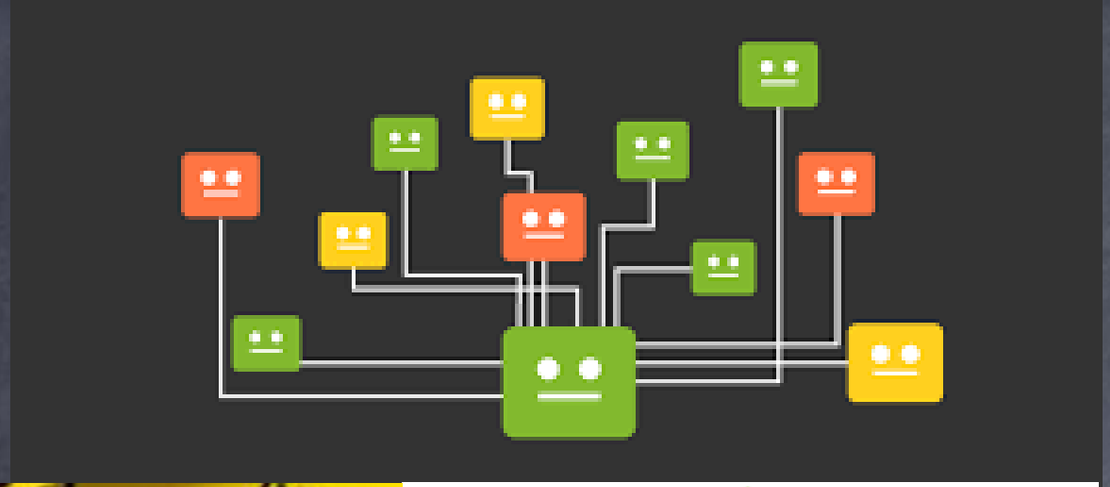


Playing with Danger: A Taxonomy and Evaluation of Threats to Smart Toys 2018

- ✓ Игрушки через Wi-Fi могут отправлять информацию о владельце в Интернет
- ✓ Через них можно прослушивать семейные разговоры, перехватывать все приходящие и исходящие сообщения
- ✓ Можно удаленно посылать игрушке различные команды
- ✓ Игрушка, войдя в доверие к ребенку, сама может начать задавать ему вопросы


Initiate
Attack
Attacker
Control
Server
Initiate Attack
Botnet
Attach Nodes
Attack Traffic
Victim


Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things



BOTNET (RO**BOT**IC **NET**WORK)
- Сеть компьютеров, которые инфицированы вредоносным ПО и удаленно контролируются злоумышленником. Предназначена для проведения DDoS-атаки

DDoS-атака (Distributed Denial of Service)
– атака, следствием которой является полное прекращение работы атакуемой компьютерной системы за счёт поступления огромного количества ложных запросов

Worms Could Spread Like Zombies via Internet of Things

IoT worm can hack Philips Hue lightbulbs, spread across cities

IoT-ботнет на базе трояна Mirai едва не лишил интернета целую страну

Next-gen IoT botnet Hajime nearly 300K strong

How hackers could use doll to open your front door

Cryptocurrency Mining Botnets Are Getting Out Of Control

Botnet Infects Half a Million Servers to Mine Thousands of Monero

Ботнет Satori атакует уязвимые фермы для майнинга

Make your own monero botnet or setup your own hidden miner installer

Coinhive – 12% организаций во всем мире

Источники угроз кибербезопасности

- Malicious Software (Malware)
- Malicious Hardware
- Covert, Subliminal, Side Channels; Backdoors
- Использование по двойному назначению технологий защиты информации (Malicious Cryptography)

Кибервойна уже идет !

Кибервойна уже идет !

Информационное противоборство в киберпространстве

Кибервойна уже идет !

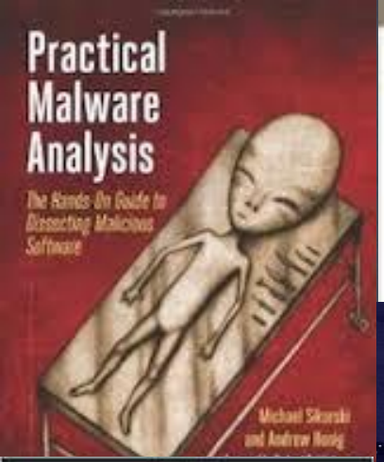
Информационное противоборство в киберпространстве

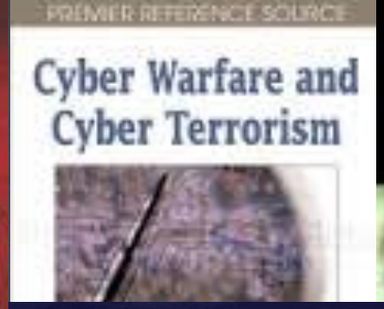
- Размещение в компьютерных сетях противника *логических бомб* (**Logic Bombs**), т.е. вредоносных программ, начинающих функционировать только при выполнении определенных условий, например, по команде извне, и *троянских программ* (**Trojans**), создающих скрытые каналы информационного воздействия или передачи информации

Кибервойна уже идет !

Информационное противоборство в киберпространстве

- Размещение в компьютерных сетях противника *логических бомб* (**Logic Bombs**), т.е. вредоносных программ, начинающих функционировать только при выполнении определенных условий, например, по команде извне, и *троянских программ* (**Trojans**), создающих *скрытые каналы* информационного воздействия или передачи информации
- Продвижение аппаратного и программного обеспечения, содержащего *уязвимости* (**Vulnerabilities**), создающие предпосылки для проведения удаленных атак, или *скрытые каналы* информационного воздействия или передачи информации (**Backdoors**)



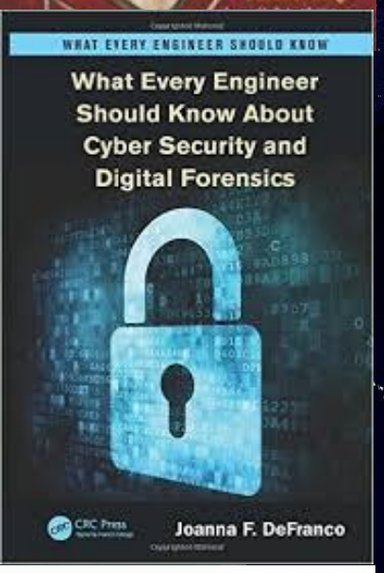


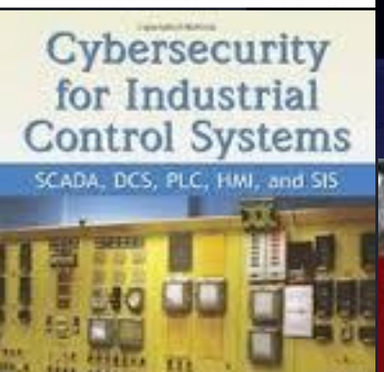
Проигравшие в кибервойне проигрывают ее навсегда, так как все их действия по исправлению ситуации будут контролироваться победившей стороной.

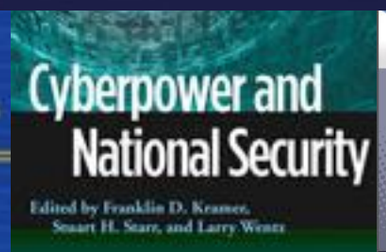
Неизвестный автор

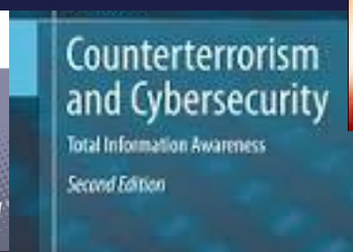
Интерактивная карта киберугроз

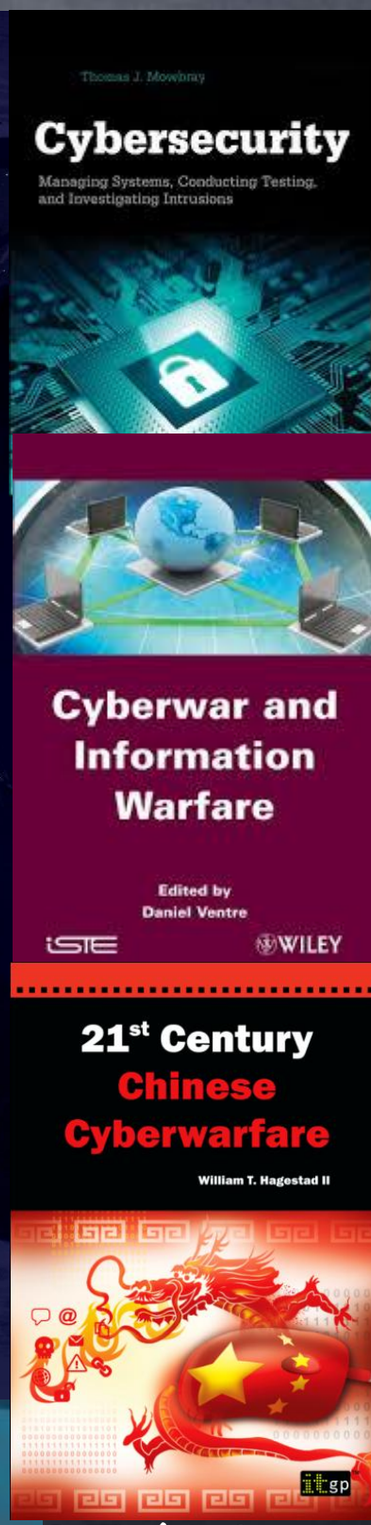
Самые атакуемые страны в мире
Россия, США, Индия, Франция, Германия











Положение дел в сфере кибербезопасности

Положение дел в сфере кибербезопасности

Сегодня

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Должно быть

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Должно быть

- Процессный подход к решению задач ЗИ → важнейшая роль принадлежит методике комплексного анализа защищенности киберсистем

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Должно быть

- Процессный подход к решению задач ЗИ → важнейшая роль принадлежит методике комплексного анализа защищенности компьютерных систем
- Решение задач ЗИ в процессе создания нового продукта, системы или технологии

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Должно быть

- Процессный подход к решению задач ЗИ → важнейшая роль принадлежит методике комплексного анализа защищенности компьютерных систем
- Решение задач ЗИ в процессе создания нового продукта, системы или технологии
- Использование проактивных методов ЗИ → защита МОЖЕТ получить преимущество перед нападением

Положение дел в сфере кибербезопасности

Сегодня

- Системный подход к решению задач защиты информации (ЗИ) → не работает !
- Решение задач ЗИ по остаточному принципу, когда продукт, система или технология уже созданы → все сводится к латанию все новых и новых «дыр»
- Использование реактивных методов ЗИ → защита находится в заведомо проигрышном положении по отношению к нападающей стороне
- Использование модели «Black Box» → не работает !

Должно быть

- Процессный подход к решению задач ЗИ → важнейшая роль принадлежит методике комплексного анализа защищенности киберсистем
- Решение задач ЗИ в процессе создания нового продукта, системы или технологии
- Использование проактивных методов ЗИ → защита МОЖЕТ получить преимущество перед нападением
- Использование моделей «Grey Box» и «White Box»

Когда защита получает преимущество перед нападением ?

Когда защита получает преимущество перед нападением ?

-> Когда нападающему непонятно поведение объекта атаки -> внесение непредсказуемости в работу средств и объектов защиты

Когда защита получает преимущество перед нападением ?

-> Когда нападающему непонятно поведение объекта атаки -> внесение непредсказуемости в работу средств и объектов защиты

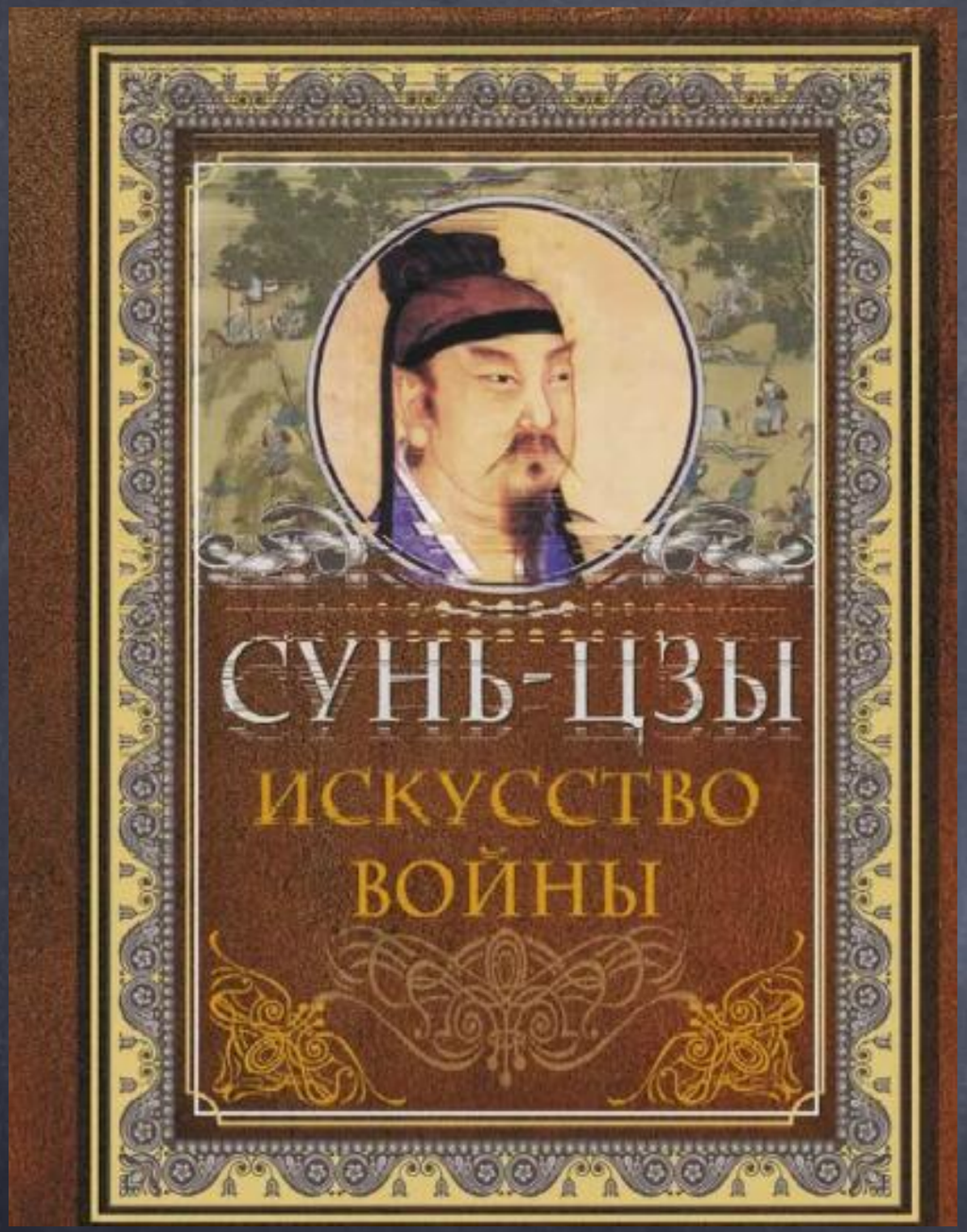
-> Когда нападающему кажется, что он понимает поведение объекта атаки, а на самом деле это не так -> создание ложных объектов атаки

Когда защита получает преимущество перед нападением ?

-> Когда нападающему непонятно поведение объекта атаки -> внесение непредсказуемости в работу средств и объектов защиты

-> Когда нападающему кажется, что он понимает поведение объекта атаки, а на самом деле это не так -> создание ложных объектов атаки

-> Нападающий вообще «не видит» объекта атаки -> стеганографические методы ЗИ



«… сто раз сразиться и сто раз победить – это не лучшее из лучшего; лучшее из лучшего – покорить чужую армию, не сражаясь»

«Война – это путь обмана. Поэтому, если ты и можешь что-нибудь, показывай противнику, будто не можешь; если ты и пользуешься чем-нибудь, показывай ему, будто ты этим не пользуешься; хотя бы ты и был близко, показывай, будто ты далеко; хотя бы ты и был далеко, показывай, будто ты близко; заманивай его выгодой; приведи его в расстройство и бери его …»

Защищенные компьютерные технологии

Защищенные компьютерные технологии

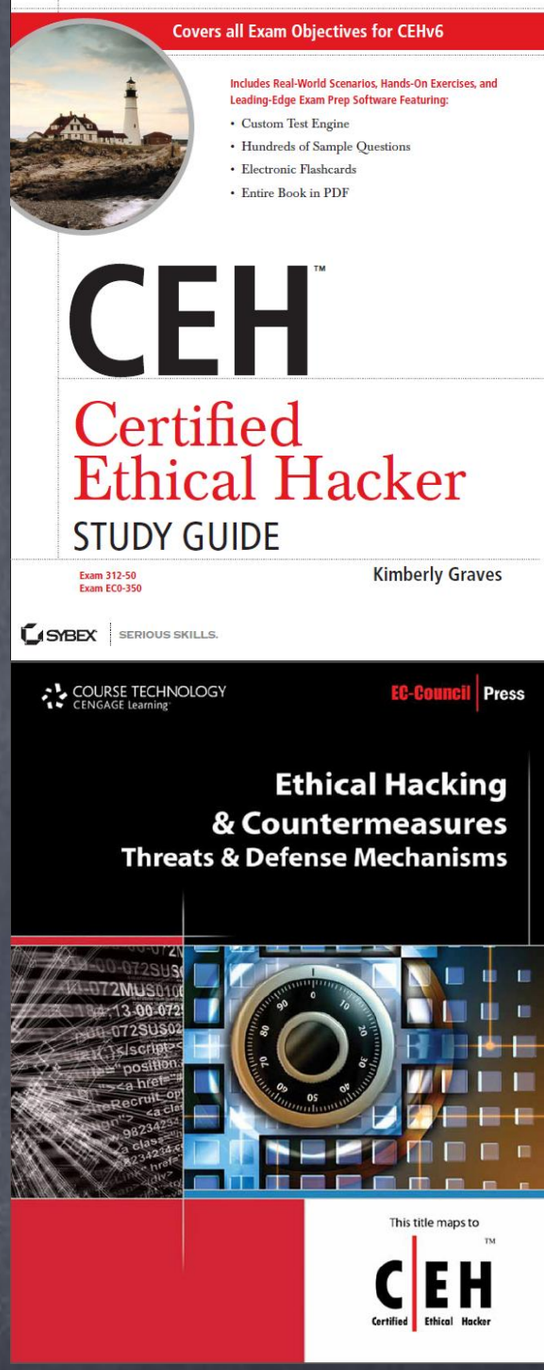
- Разработка и исследование стохастических методов ЗИ в компьютерных системах и сетях

Защищенные компьютерные технологии

- Разработка и исследование стохастических методов ЗИ в компьютерных системах и сетях
- Выявление тенденций развития механизмов проведения атак на компьютерные системы. Опережающее совершенствование методов и средств защиты от них

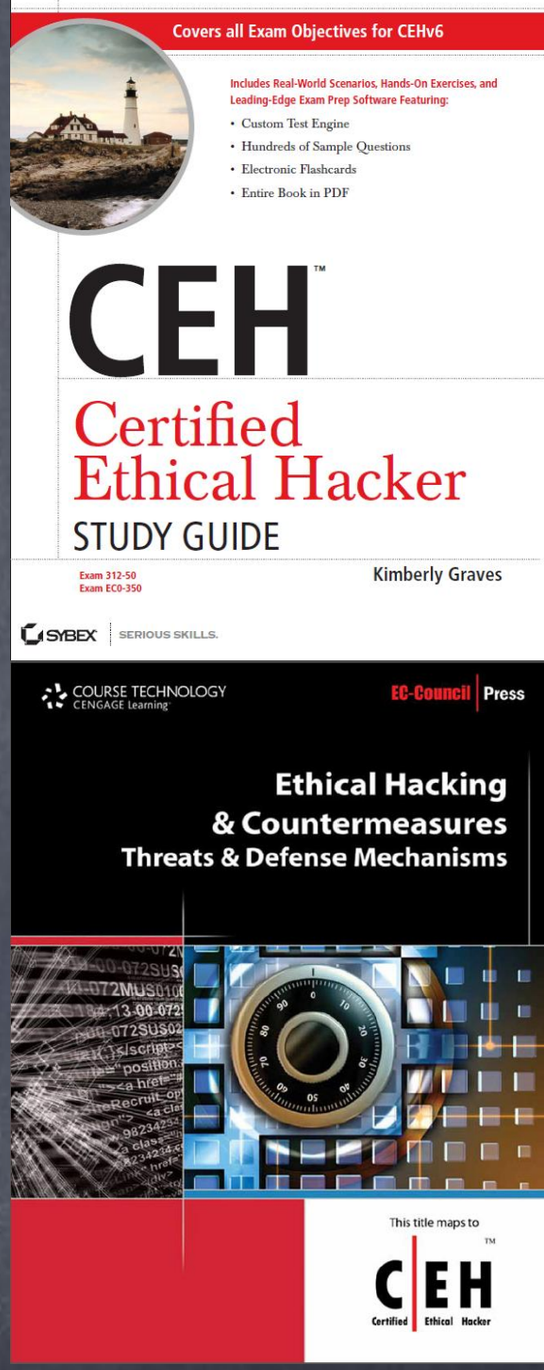
Защищенные компьютерные технологии

- Разработка и исследование стохастических методов ЗИ в компьютерных системах и сетях
- Выявление тенденций развития механизмов проведения атак на компьютерные системы. Опережающее совершенствование методов и средств защиты от них
- Разработка методики комплексного анализа защищенности критически важных компьютерных систем (элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО)

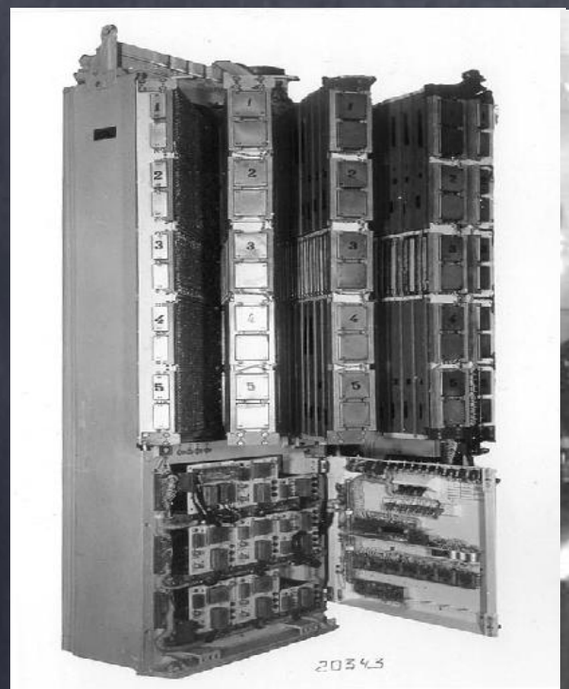


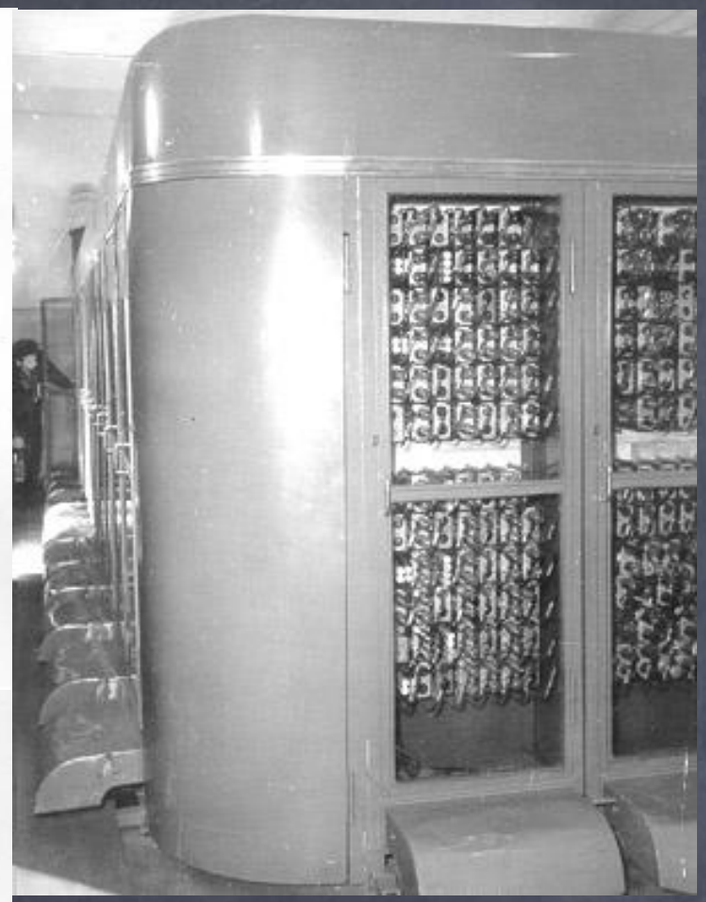
Защищенные компьютерные технологии

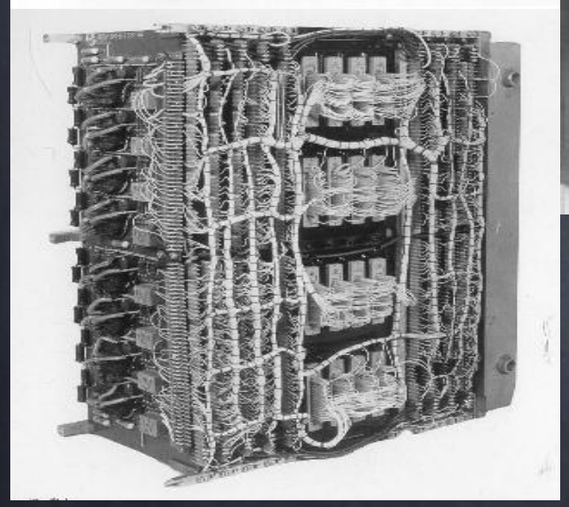
- Разработка и исследование криптографических методов ЗИ в компьютерных системах и сетях
- Выявление тенденций развития механизмов проведения атак на компьютерные системы. Опережающее совершенствование методов и средств защиты от них
- Разработка методики комплексного анализа защищенности критически важных компьютерных систем (элементная база, архитектура, системное ПО, сетевое ПО, прикладное ПО)
- Обеспечение технологической независимости



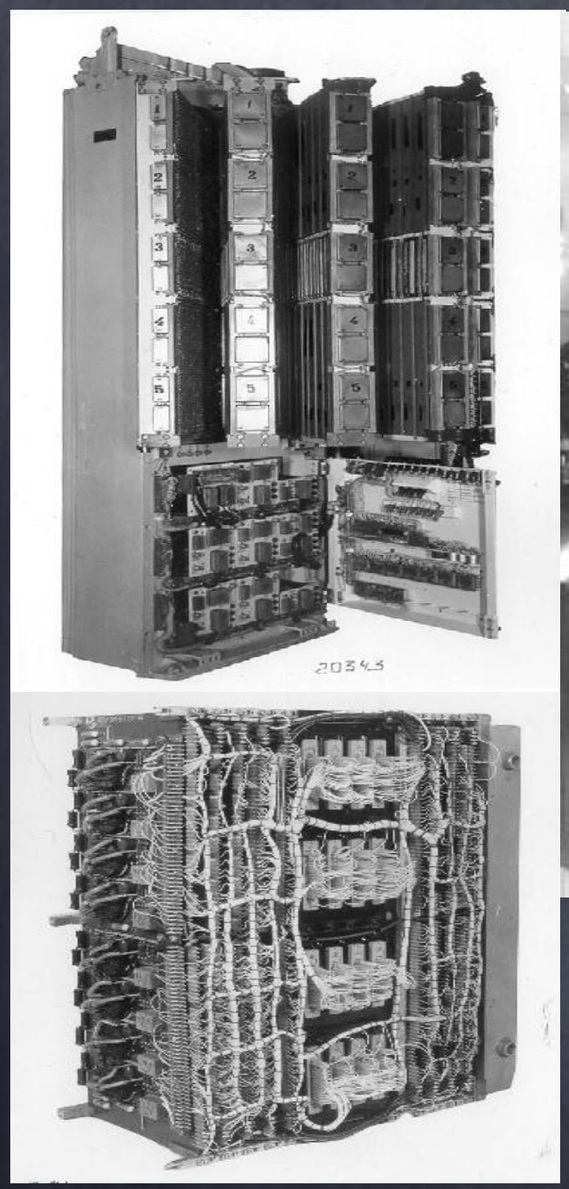
Обеспечение технологической независимости - реальная задача !







Обеспечение технологической независимости - реальная задача !

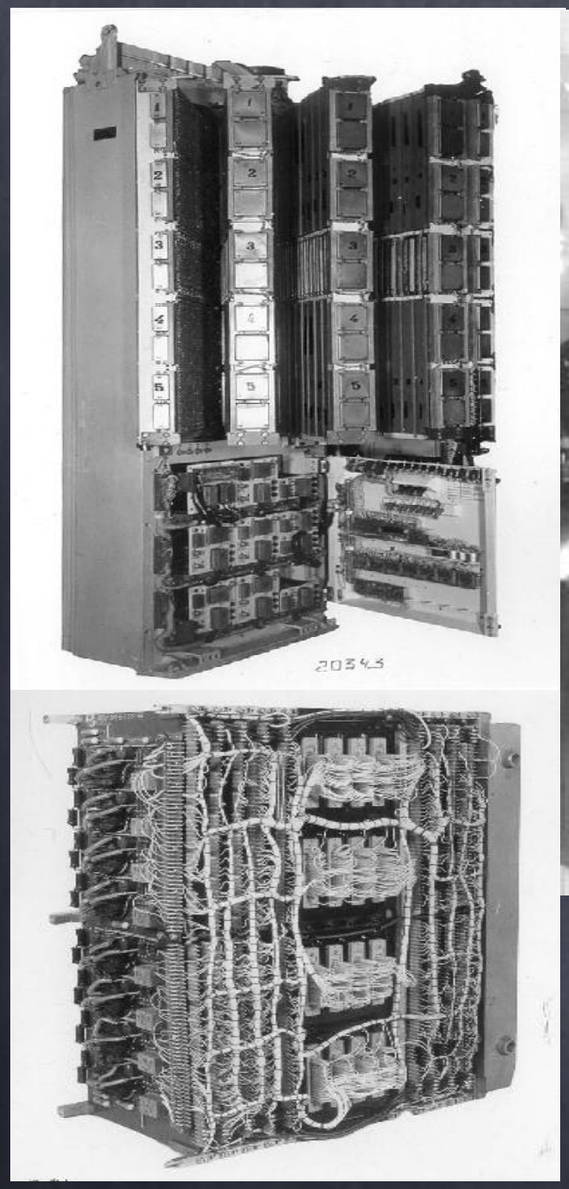


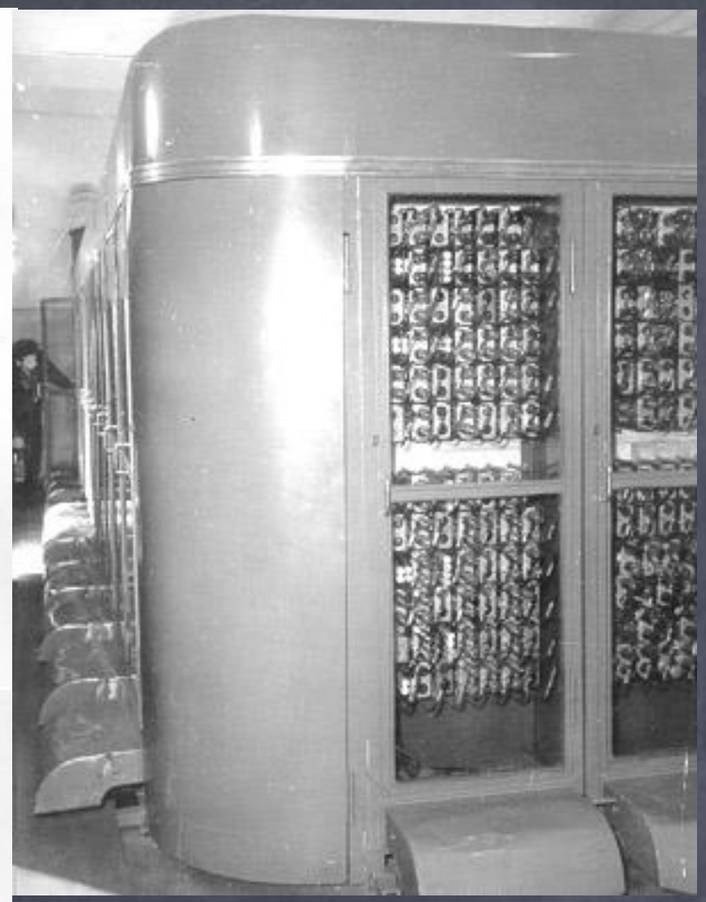
Кто придумал Linux? -> МСВС ->
-> Арамид (РФЯЦ-ВНИИЭФ) ->
-> Саров -> План Дропшот

ИИ -> Где в компьютере мозг? ->
-> Лучший в мире лабораторный практикум

МЦСТ -> 2012 -> ТБВ Эльбрус

Обеспечение технологической независимости – реальная задача !





Безопасность слишком важна, чтобы пренебрегать ею.
Но заботиться о безопасности – значит быть
безжалостным во многих других областях. …
Невозможно обеспечить «чуть-чуть» безопасности.
… все должно быть принесено в жертву безопасности.

Н. Фергюсон, Б. Шнайер.
Практическая криптография.

10 - 90

The End

The Questions are Welcome!

Кафедра № 12
Компьютерные системы и технологии

Стохастические методы защиты информации

Иванов М.А.

Москва 2025

Причины трудоемкости решения задач защиты информации

-> Информационная война
-> Политика коммерческих IT-компаний
-> **Повсеместное использование криптографии**
-> Уязвимые IT-технологии
-> Сложность информационных систем
-> Все большее отстранение пользователей от реальных процессов обработки информации и управления
-> Человеческий фактор

Часть 1
Стохастические методы ЗИ

Когда защита получает преимущество перед нападением ?

-> Защита всегда отстает

-> У нападения всегда есть резерв времени

-> Защита практически никогда не знает, кто ее будет атаковать и когда, какие возможности и какие цели у атакующих

-> Новые уязвимые IT-технологии дают в руки атакующих все новые и новые возможности

-> Механизмы проведения атак постоянно совершенствуются

⬇

Защищаться намного сложнее, чем атаковать

⬇

Положение защиты похоже на безнадежное

Когда защита получает преимущество перед нападением ?

-> Когда нападающему непонятно поведение объекта атаки -> внесение непредсказуемости в работу средств и объектов защиты

-> Когда нападающему кажется, что он понимает поведение объекта атаки, а на самом деле это не так -> создание ложных объектов атаки

-> Нападающий вообще «не видит» объекта атаки -> стеганографические методы ЗИ

Когда защита получает преимущество перед нападением ?

↓

Когда нападающему непонятно поведение объекта атаки
-> внесение непредсказуемости в работу средств
и объектов защиты

↓

Генераторы псевдослучайных чисел (ГПСЧ)

↓

Стохастические методы защиты информации

↓

Это универсальные методы !

ГПСЧ vs ГСЧ

-> Ограниченные возможности по обеспечению требуемых статистических характеристик

-> Физические источники случайности подвержены влиянию дестабилизирующих факторов

-> Отсутствие возможности повторной генерации ПСП

-> Часто применяются уникальные методы схемотехнического построения, не допускающие программной реализации

ГПСЧ

-> Непредсказуемость
-> Статистическая безопасность
-> Гарантированно большой период
-> Эффективная программная
и аппаратная реализация
-> Удобство интегрального исполнения

-> Хеш-генератор – это ГПСЧ со входом
(см. Sponge)

Помехоустойчивый код + ГПСЧ ->
-> Стохастический код -> Универсальная защита информации, пересылаемой по каналу связи

Шифр + ГПСЧ -> Вероятностный шифр ->
-> Вероятностная криптография

УВВ + ГПСЧ -> Плавающий протокол взаимодействия процессора и УВВ

Компьютерный вирус + ГПСЧ ->
-> Полиморфный вирус -> Метаморфный вирус

Эксплойт + ГПСЧ -> Полиморфный эксплойт ->
-> AdmMutate

КМЗИ и СМЗИ – это частные случаи стохастических методов ЗИ !!!

ЭВМ + ГПСЧ

↓

Стохастическая вычислительная машина !!!

Главная цель:
Компьютерная система, которая постоянно и непредсказуемо меняется

↓

Защита от атак, основанных
на эксплуатации уязвимостей ПО,
(Morpheus, SOFIA, CHERI, ТБВ Эльбрус …)

Примеры стохастических методов ЗИ

Software

-> Software Obfuscation
-> ASLR -> NOP Tube
-> ISR (Instruction Set Randomization)
-> CFI (Control Flow Integrity) -> SOFIA
-> MTD (Moving Target Defense) -> Morpheus

Hardware

-> Built-in Self Testing
-> Design Obfuscation
-> Logic Encryption
-> N-variant Logic
-> Hidden Functions
-> PUF (Physical Unclonable Functions)

Шаг № 1

-> Исследование современных механизмов проведения атак на компьютерные системы (Code Reuse Attacks -> ROP, JOP, …)

-> Разработка технологии безопасного программирования

Примеры уязвимого кода -> Примеры эксплуатации -> -> Примеры безопасного кода (по каждой уязвимости)

-> Исследование современных методов защиты от атак, основанных на эксплуатации уязвимостей ПО (MTD, CFI, MTE, …),

-> Анализ существующих технических решений (Morpheus, SOFIA, CHERI, …), поиск направлений их совершенствования

Часть 2
Особенности криптографии как науки

Особенности криптографии как науки

Криптография как математическая наука

vs

Криптография как инженерная дисциплина

Уязвимости реализации КА

Алгоритмические атаки на КА

Криптографические бэкдоры

Криптографические скрытые каналы

Криптография как математическая наука
vs
Криптография как инженерная дисциплина

- ✓ Уязвимости реализации КА
- ✓ Алгоритмические атаки на КА
- ✓ Криптографические бэкдоры
- ✓ Криптографические скрытые каналы
- ✓ Setup-атаки
- ✓ Клептографические атаки

Криптография

Криптография

-> Криптография может решить практически любую задачу, связанную с защитой информации

Криптография

-> Криптография может решить практически любую задачу, связанную с защитой информации

-> Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана

Криптография

-> Криптография может решить практически любую задачу, связанную с защитой информации

-> Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана

-> Криптография – технология двойного назначения и может использоваться не только для защиты, но и для нападения

Криптография

-> Криптография может решить практически любую задачу, связанную с защитой информации

-> Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана

-> Криптография – технология двойного назначения и может использоваться не только для защиты, но и для нападения

-> Криптография сложнее, чем кажется

Криптография

-> Криптография может решить практически любую задачу, связанную с защитой информации

-> Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана

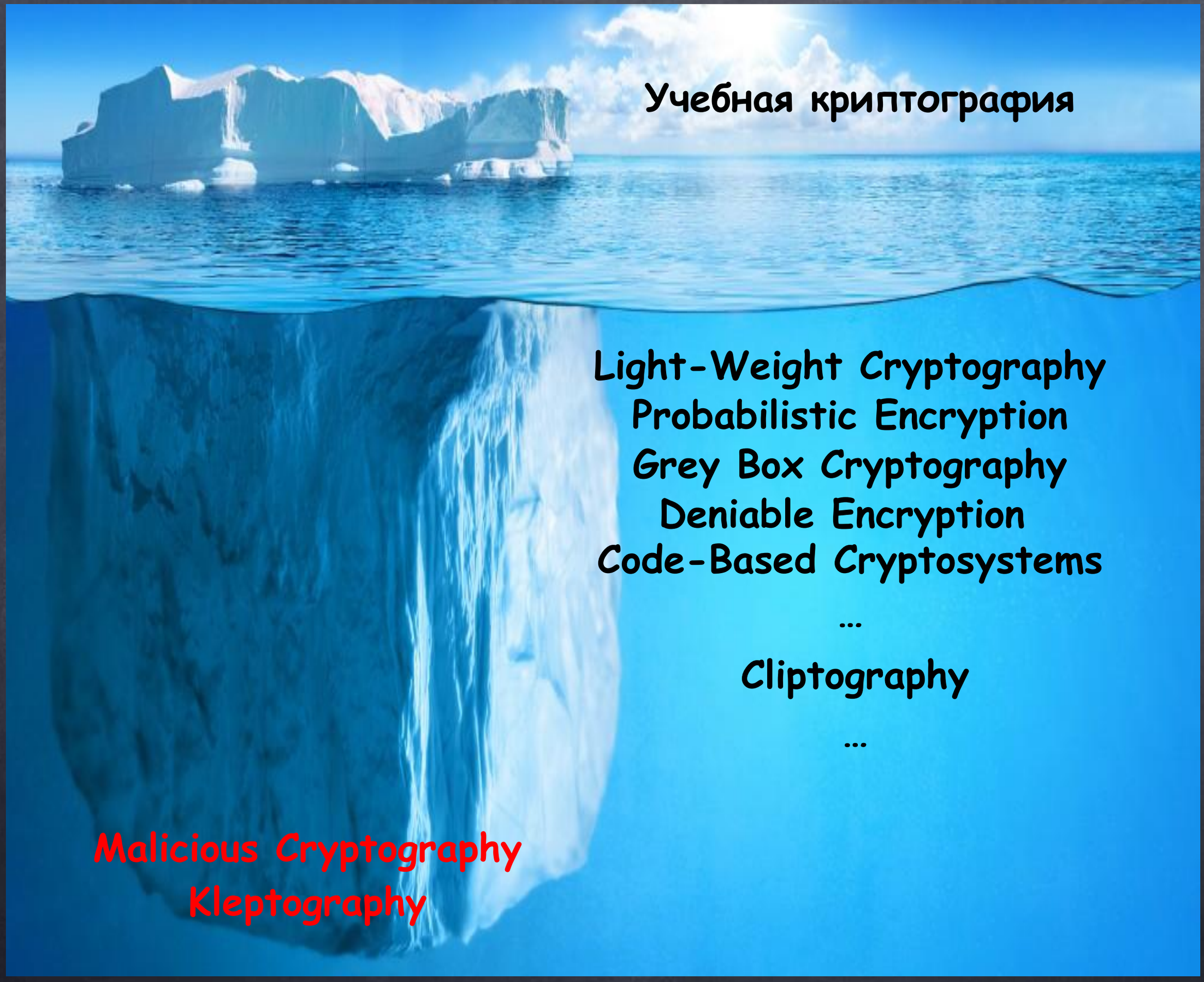
-> Криптография – технология двойного назначения и может использоваться не только для защиты, но и для нападения

-> Криптография сложнее, чем кажется

-> Криптография опасна тем, что очень часто создает лишь видимость безопасности

Криптография

- Криптография может решить практически любую задачу, связанную с защитой информации (ЗИ)
- Стойкость ни одного криптографического алгоритма, который реально используется на практике, строго математически не доказана
- Криптография – технология двойного назначения и может использоваться не только для защиты, но и для нападения
- Криптография сложнее, чем кажется
- Криптография опасна тем, что очень часто создает лишь видимость безопасности
- Повсеместное использование криптографии – одна из причин трудоемкости решения задач ЗИ


Учебная криптография
Light-Weight Cryptography
Probabilistic Encryption
Grey Box Cryptography
Deniable Encryption
Code-Based Cryptosystems
…
Cliptography
…
Malicious Cryptography
Kleptography

Без криптографии
цифровую экономику (ЦЭ)
не построить

Главная проблема ЦЭ – обеспечение
цифрового доверия !

Главное препятствие
на пути развития
цифровой экономики
- нерешенная проблема
кибербезопасности !

Задачи, решаемые криптографическими методами

- Обеспечение секретности (конфиденциальности) информации
- Обеспечение аутентичности (подлинности) субъектов информационного взаимодействия (абонентов)
- Обеспечение аутентичности (целостности, подлинности) объектов информационного взаимодействия (сообщений, документов, массивов данных)
- Защита авторских прав, прав собственников информации
- Обеспечение неотслеживаемости информации
- Разграничение доступа
- Разделение доступа

Классическая криптография:
криптографические механизмы защиты информации

-> Криптосистемы с секретным ключом,
быстродействующие, но требующие
наличия надежных каналов связи
для обмена ключами
и не обеспечивающие юридической
значимости пересылаемых
электронных документов

-> Хеш-функции (ХФ)

-> Генераторы псевдослучайных чисел (ГПСЧ)



ГПСЧ – основа стохастических методов
защиты информации !

1948 г.
К. Шеннон
Теория связи
в секретных системах

СССР: В.И. Шестаков, В.А. Котельников

Современная криптография:
криптографические механизмы защиты информации

-> Криптосистемы с открытым ключом, не требующие наличия надежных каналов связи для обмена ключами

-> Схемы гибридного шифрования

-> Протоколы выработки общего секретного ключа

-> Протоколы электронной подписи (ЭП): классическая ЭП, групповая подпись, неотвергаемая подпись, слепая подпись, одноразовая кольцевая подпись и пр.

-> Протоколы аутентификации (проверки подлинности) удаленных абонентов, в том числе протоколы доказательства с нулевым разглашением знаний (**Zero Knowledge Proofs**)

-> Протоколы привязки к биту (**Bit Commitment**)

-> Протоколы правдоподобного отрицания

-> Протоколы разделения секрета и ряд других, менее известных

1976 г.
У. Диффи, М. Хеллман
Новые направления в криптографии
Р. Меркль

Криптография. История первая

Энигма

А. Тьюринг

1912 - 1954

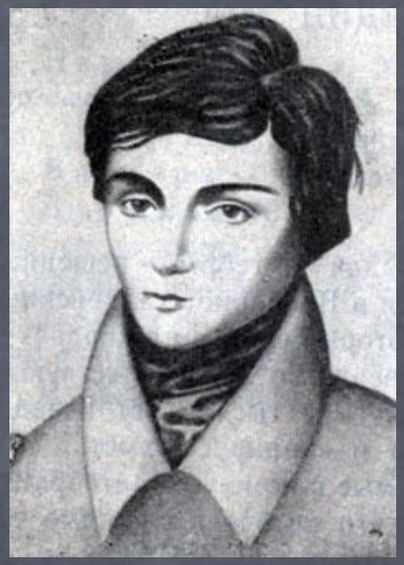
Bombe

Криптография. История первая

Энигма

А. Тьюринг
1912 - 1954

Ф. Бэкон
1561-1626



Э. Галуа
1811-1832

Р. Ривест

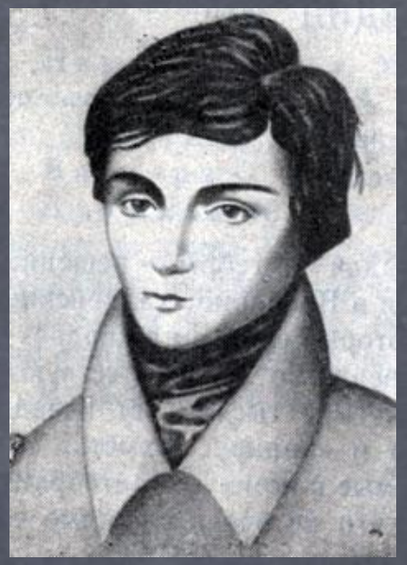
Bombe

Криптография. История первая

Энигма

А. Тьюринг
1912 - 1954

Ф. Бэкон
1561-1626



Э. Галуа
1811-1832

Р. Ривест

Bombe

Дж. Эллис, К. Кокс и М. Уильямсон
Сотрудники ШКПС Великобритании
Авторы NSE

Криптография. История вторая. Государственные стандарты

-> США: DES (1974 г.) → AES (2001 г.)

Криптография. История вторая. Государственные стандарты

-> США: DES (1974 г.) → AES (2001 г.)

-> Россия:

ГОСТ 28147-89 → Кузнечик, Магма (2016 г.)

Криптография. История вторая. Государственные стандарты

-> США: DES (1974 г.) → AES (2001 г.)

-> Россия:
ГОСТ 28147-89 → Кузнечик, Магма (2016 г.)

-> Япония:
FEAL → FEAL-2 → ... → FEAL-8

Криптография. История вторая. Государственные стандарты

-> США: DES (1974 г.) → AES (2001 г.)

-> Россия:

ГОСТ 28147-89 → Кузнечик, Магма (2016 г., 2018 г.)

-> Япония:

FEAL -> FEAL-2 -> ... -> FEAL-8

-> Китай:

SM4 (2006 г.)

Криптография. История третья.

Ада Лавлейс (1815-1852)

Автор описания вычислительной машины,
проект которой был разработан
Чарльзом Бэббиджем.
Составила первую в мире программу
для этой машины.
Считается первым программистом

Ленор Блюм

BBS-generator

Шафи Гольдвассер

Probabilistic Encryption

Криптография. История четвертая.
Шифр Ф. Бэкона

- ✓ Двоичная СС (двухлитерное кодирование)
- ✓ Операция замены
- ✓ Имеет вероятностные свойства
- ✓ Первый в мире отрицаемый шифр
- ✓ Первый в мире шифр со стеганографическими свойствами
- ✓ Существует много путей его модификации и совершенствования

Сим-волы ал-фа-вита	Ключевая информация			
	Двухли-терный код	k1	k2	k3
1	2	3	4	5
A	*abbbb*	*a*	*b*	*b*
B	*babbb*	*a*	*a*	*b*
C	*bbabb*	*a*	*b*	*a*
D	*abbab*	*a*	*a*	*b*
E	*babba*	*a*	*b*	*a*
F	*ababb*	*a*	*a*	*a*
G	*aabab*	*a*	*b*	*b*
H	*baaba*	*a*	*a*	*b*
I	*bbaab*	*a*	*b*	*b*
J	*abbaa*	*a*	*a*	*a*
K	*aabba*	*a*	*b*	*a*
L	*aaabb*	*a*	*a*	*b*
M	*aaaab*	*a*	*b*	*a*
N	*aaaaa*	*b*	*a*	*b*
O	*baaaa*	*b*	*b*	*b*
P	*bbaaa*	*b*	*a*	*a*
Q	*bbbaa*	*b*	*b*	*a*
R	*abbba*	*b*	*a*	*b*
S	*aabbb*	*b*	*b*	*b*
T	*baabb*	*b*	*a*	*a*
U	*abaab*	*b*	*b*	*b*
V	*aabaa*	*b*	*a*	*a*
W	*aaaba*	*b*	*b*	*a*
X	*baaab*	*b*	*a*	*a*
Y	*abaaa*	*b*	*b*	*b*

Шифр Ф. Бэкона. Режим 1 Отрицаемый шифр

m = CAT

Зашифрование

1-й шаг: *c* = *bbabb abbbb baabb*

2-й шаг: *c* = NOCVW ARTVZ PFGVY

Криптограмма

c = NOCVW ARTVZ PFGVY

Сим-волы ал-фа-вита	Ключевая информация			
	Двухли-терный код	k1	k2	k3
1	2	3	4	5
A	abbbb	a	b	b
B	babbb	a	a	b
C	bbabb	a	b	a
D	abbab	a	a	b
E	babba	a	b	a
F	ababb	a	a	a
G	aabab	a	b	b
H	baaba	a	a	b
I	bbaab	a	b	b
J	abbaa	a	a	a
K	aabba	a	b	a
L	aaabb	a	a	b
M	aaaab	a	b	a
N	aaaaa	b	a	b
O	baaaa	b	b	b
P	bbaaa	b	a	a
Q	bbbaa	b	b	a
R	abbba	b	a	b
S	aabbb	b	b	b
T	baabb	b	a	a
U	abaab	b	b	b
V	aabaa	b	a	a
W	aaaba	b	b	a
X	baaab	b	a	a
Y	abaaa	b	b	b

m = CAT

Зашифрование

1-й шаг: *c* = *bbabb abbbb baabb*

2-й шаг: *c* = NOCVW ARTVZ PFGVY

Криптограмма

c = NOCVW ARTVZ PFGVY

Расшифрование 1 (k1)

1-й шаг: *m* = *bbabb abbbb baabb*

2-й шаг: *m* = CAT

Сим-волы ал-фа-вита	Ключевая информация			
	Двухли-терный код	k1	k2	k3
1	2	3	4	5
A	abbbb	a	b	b
B	babbb	a	a	b
C	bbabb	a	b	a
D	abbab	a	a	b
E	babba	a	b	a
F	ababb	a	a	a
G	aabab	a	b	b
H	baaba	a	a	b
I	bbaab	a	b	b
J	abbaa	a	a	a
K	aabba	a	b	a
L	aaabb	a	a	b
M	aaaab	a	b	a
N	aaaaa	b	a	b
O	baaaa	b	b	b
P	bbaaa	b	a	a
Q	bbbaa	b	b	a
R	abbba	b	a	b
S	aabbb	b	b	b
T	baabb	b	a	a
U	abaab	b	b	b
V	aabaa	b	a	a
W	aaaba	b	b	a
X	baaab	b	a	a
Y	abaaa	b	b	b

m = CAT

Зашифрование

1-й шаг: *c* = *bbabb abbbb baabb*

2-й шаг: *c* = NOCVW ARTVZ PFGVY

Криптограмма

c = NOCVW ARTVZ PFGVY

Расшифрование 2 (k2)

1-й шаг: *m´ = abbab baaaa aabab*

2-й шаг: *m´* = DOG

Сим-волы ал-фа-вита	Ключевая информация			
	Двухли-терный код	k1	k2	k3
1	2	3	4	5
A	abbbb	a	b	b
B	babbb	a	a	b
C	bbabb	a	b	a
D	abbab	a	a	b
E	babba	a	b	a
F	ababb	a	a	a
G	aabab	a	b	b
H	baaba	a	a	b
I	bbaab	a	b	b
J	abbaa	a	a	a
K	aabba	a	b	a
L	aaabb	a	a	b
M	aaaab	a	b	a
N	aaaaa	b	a	b
O	baaaa	b	b	b
P	bbaaa	b	a	a
Q	bbbaa	b	b	a
R	abbba	b	a	b
S	aabbb	b	b	b
T	baabb	b	a	a
U	abaab	b	b	b
V	aabaa	b	a	a
W	aaaba	b	b	a
X	baaab	b	a	a
Y	abaaa	b	b	b

m = CAT

Зашифрование

1-й шаг: *c* = *bbabb abbbb baabb*

2-й шаг: *c* = NOCVW ARTVZ PFGVY

Криптограмма

c = NOCVW ARTVZ PFGVY

Расшифрование 3 (k3)

1-й шаг: *m″ = bbaaa bbaab aabab*

2-й шаг: *m″* = PIG

Шифр Ф. Бэкона. Режим 2 Стеганографическое сокрытие информации

1	2
A	*abbbb*
B	*babbb*
C	*bbabb*
D	*abbab*
E	*babba*
F	*ababb*
G	*aabab*
H	*baaba*
I	*bbaab*
J	*abbaa*
K	*aabba*
L	*aaabb*
M	*aaaab*
N	*aaaaa*
O	*baaaa*
P	*bbaaa*
Q	*bbbaa*
R	*abbba*
S	*aabbb*
T	*baabb*
U	*abaab*
V	*aabaa*
W	*aaaba*
X	*baaab*
Y	*abaaa*

m = PASSWORD

m = bbaaa abbbb aabbb aabbb aaaba baaaa …

Пустой контейнер:

стеганография скрывает сам факт наличия секретной информации

Сокрытие информации:

1) bbaaa abbbb aabbb aabbb aaaba baaaa abbba abbab

2) Стега ногра фияск рывае тсамф актна личия секре

3) стЕГА Ногра ФИяск РЫІвае ТСАмФ аКТНА ЛичиЯ СекРе

4) стЕГАНограФИя скРЫІваеТ Сам ФаКТ НАЛичиЯ СекРетной информации

Заглавная буква – литера a
Строчная буква – литера b

The End

The Questions are Welcome !