Кафедра № 12 МИФИ

Лекции 1-2

Защищенные компьютерные технологии: миф или реальность?

Иванов М.А.

Москва, 2023

Иванов Михаил Александрович

maivanov@mephi.ru

Discord
https://discord.gg/TW6TaSj
Канал «Защита информации»

aha.ru/~msa

Задания для самостоятельной работы

1) Return-Oriented Programming (ROP).
2) Jump Oriented Programming (JOP).
3) Технология безопасного программирования (Buffer Overflow*, Race Condition*, Integer Overflow*, Heap Overflow, Double Free, …).
4) Moving Target Defense -> Morpheus (патенты США)
5) Control Flow Integrity -> SOFIA (патенты США)
6) Memory Tagging Extension -> CHERI (патенты).
7) Криптографические бэкдоры в асимметричных КС (Knapsack, RSA, …).
8) Криптографические бэкдоры в блокчейне.
9) Криптографические бэкдоры в симметричных КС.
10) SETUP-атаки.
11) PUF.
12) Лабораторный практикум по ЗИ (GF, программные модели PRNG, новые статистические тесты, шифр Бэкона, …)

Что будем изучать?

1) Основы криптологии.
2) Криптосистемы с секретным ключом (ГОСТ 28147-89, AES, Кузнечик).
3) Криптосистемы с открытым ключом (RSA, Knapsack, Shamir, ElGamal).
4) Теория полей Галуа (математические и схемотехнические основы).
5) Криптографические протоколы.
6) Криптографические бэкдоры.
7) Основы теории ГПСЧ.
8) Основы теории хеш-функций.
9) Стохастические методы ЗИ.
10) Вероятностная криптография.
11) Многомерные криптоалгоритмы.
12) Технология Logic Encryption.
13) Программные средства скрытого информационного воздействия.
14) Основы теории кодирования. Стохастическое кодирование.
15) Биткоин.

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

Основной принцип информационной войны:
"Доказанная взаимосвязь несуществующих событий становится законом, определяющим поведение существующих субъектов".
С.П. Расторгуев

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

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

- ???

В конце 2020 года к Интернету было подключено более 200 миллиардов устройств

Главные угрозы кибербезопасности

2016 – Фишинг

2017 - Вирусы-вымогатели

2018 – Криптоджекинг

2019 – APT-атаки, эксплуатация аппаратных уязвимостей

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

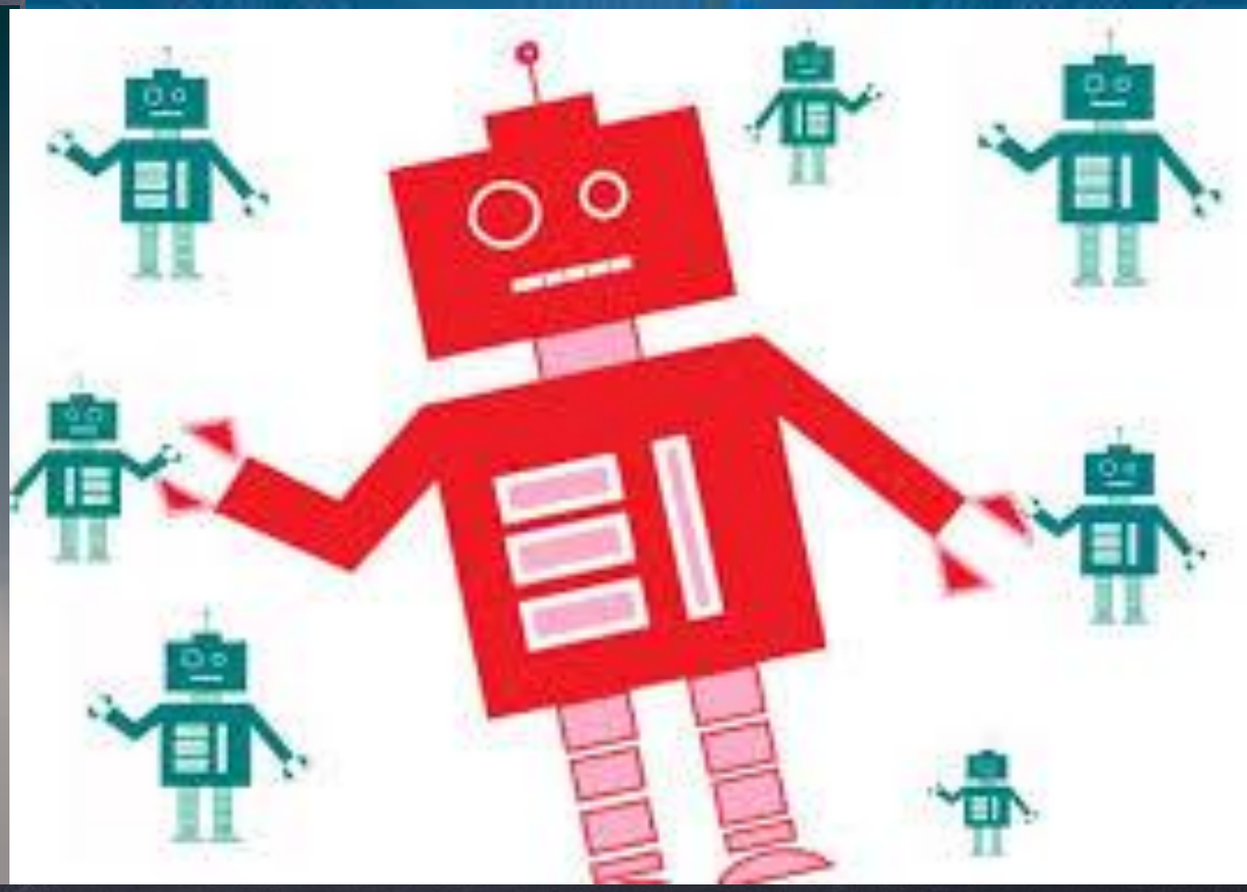
→ поиск уязвимостей ПО → участились случаи обнаружения разрушающих программных воздействий (РПВ), использующих уязвимости нулевого дня (**Zero Day Vulnerabilities**)

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

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

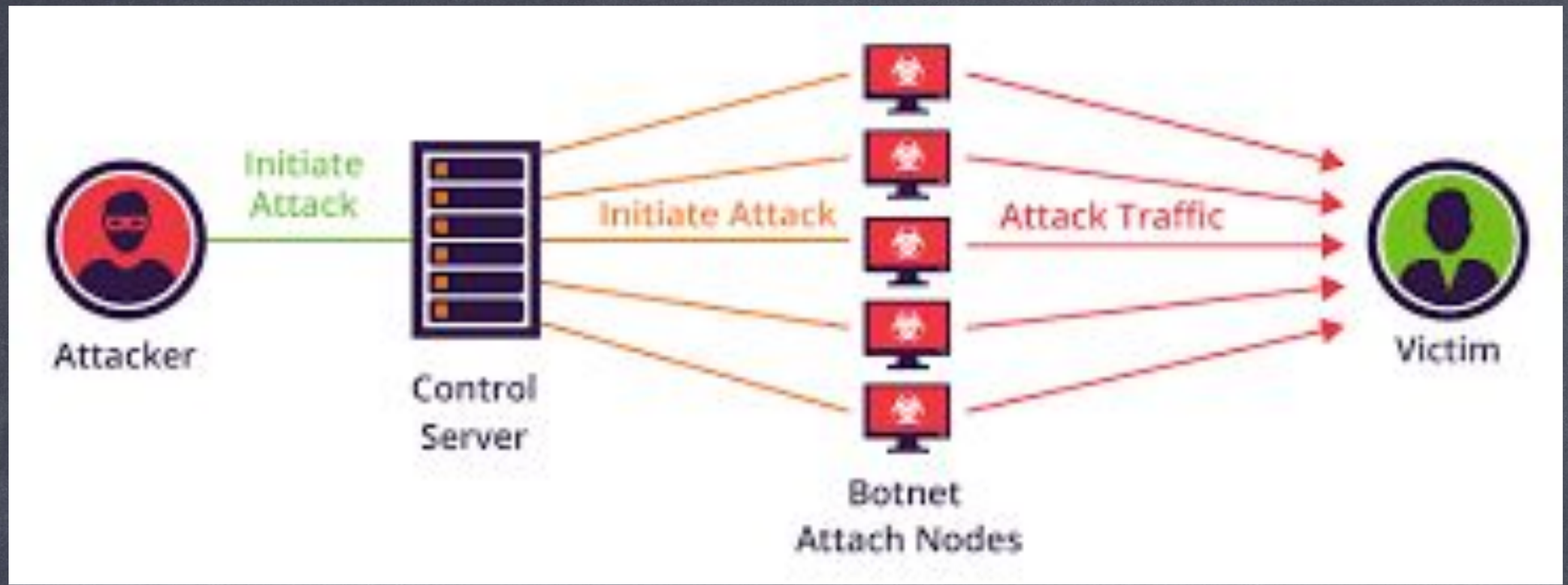
- Разрушение систем управления.
  Результат – потеря контроля над КФС
- Подмена алгоритма функционирования
- Воздействие на поведение человека посредством искажения информации, получаемой им от КФС
- Подмена сигналов GPS/Глонасс мобильной КФС → полная потеря работоспособности, поскольку изменены координаты 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

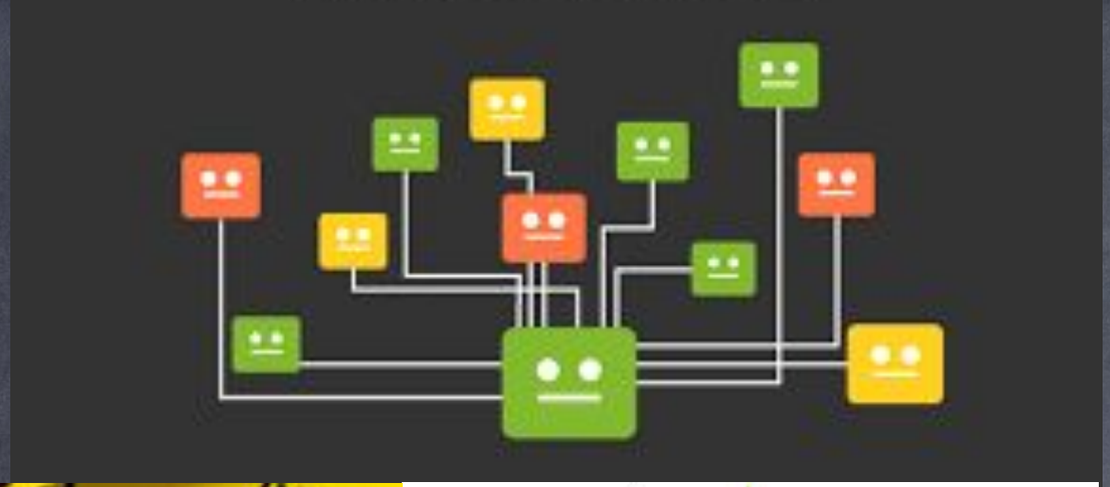


Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys

- 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
Attack Traffic
Victim
Botnet
Attach Nodes


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 (2016)

IoT worm can hack Philips Hue lightbulbs, spread across cities (2016)

IoT-ботнет на базе трояна Mirai едва не лишил интернета целую страну (2016)

Next-gen IoT botnet Hajime nearly 300K strong (2017)

How hackers could use doll to open your front door (2017)

Cryptocurrency Mining Botnets Are Getting Out Of Control (2018)

Botnet Infects Half a Million Servers to Mine Thousands of Monero (2018)

Ботнет Satori атакует уязвимые фермы для майнинга (2018)

Make your own monero botnet or setup your own hidden miner installer (2018)

Исследование: криптоджекинг в 13-й раз занял первое место в списке киберугроз (2019)

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 !

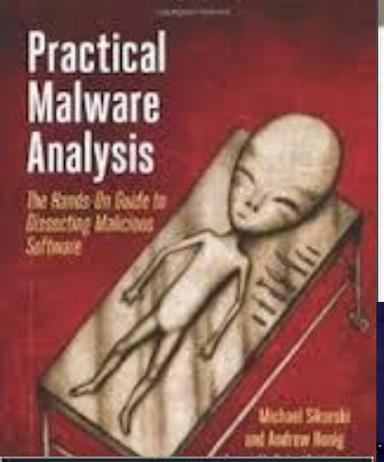
Информационное противоборство в киберпространстве

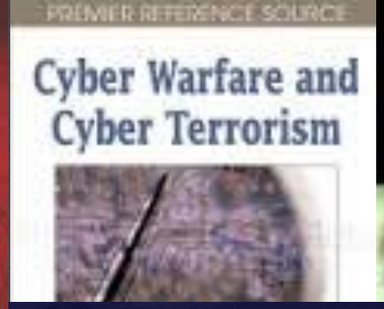
- Размещение в компьютерных сетях противника *логических бомб* (**Logic Bombs**), т.е. вредоносных программ, начинающих функционировать только при выполнении определенных условий, например, по команде извне, и *троянских программ* (**Trojans**), создающих скрытые каналы информационного воздействия или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



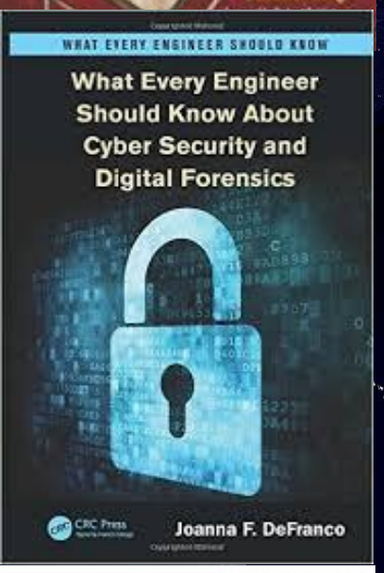


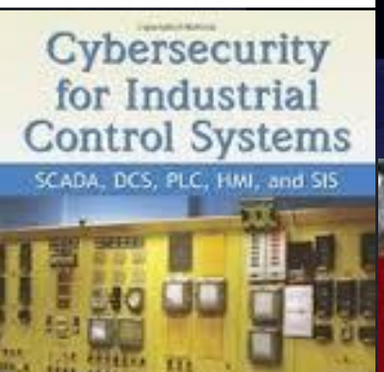
Проигравшие в кибервойне проигрывают ее навсегда, так как все их действия по исправлению ситуации будут контролироваться победившей стороной.

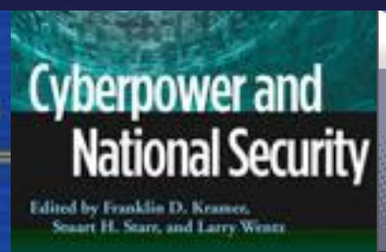
Неизвестный автор

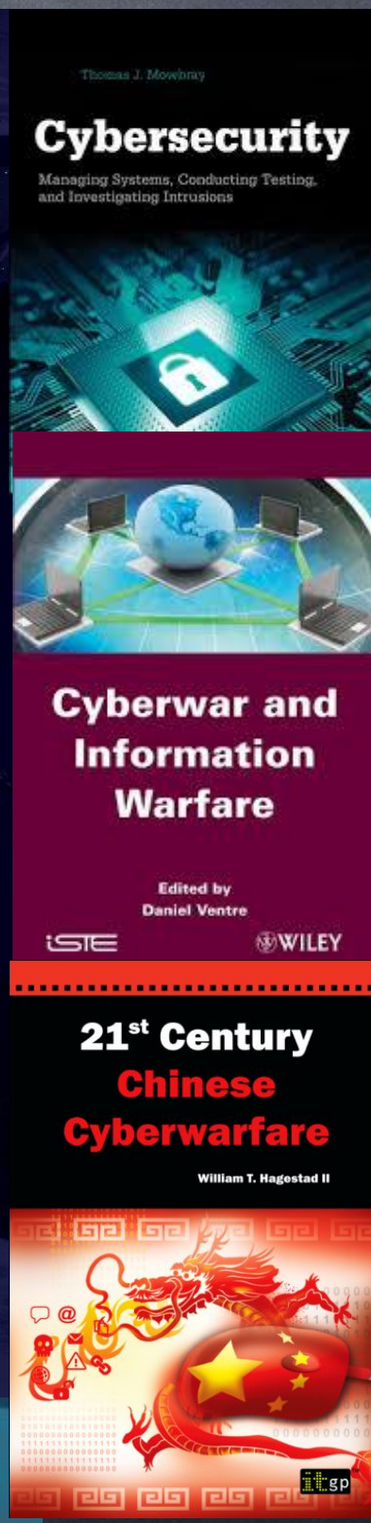
Интерактивная карта киберугроз

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 киберсистем
- 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 киберсистем
- 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 компьютерных систем
- 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 неопределенности в работу средств
  и объектов защиты

Когда защита получает преимущество перед нападением ?

- Когда нападающему непонятно поведение объекта атаки
  → внесение неопределенности 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 неопределенности 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 защиты информации

Стохастические методы ЗИ

⬇

ГПСЧ + хеш-генераторы

⬇

ГПСЧ vs ГСЧ

ГПСЧ + компьютерный вирус,
ГПСЧ + эксплойт

ГПСЧ + помехоустойчивый код,
ГПСЧ + шифр,
ГПСЧ + процессор

Технологии

Random Testing
Built-in Self Testing
Hidden Functions
N-variant Logic
Logic Encryption
Design Obfuscation

Polymorphism
Software Obfuscation
ASLR
Instruction Set Randomization

Moving Target Defense
Control Flow Integrity
Memory Tagging Extension
ТБВ Эльбрус

Защищенные компьютерные технологии

Защищенные компьютерные технологии

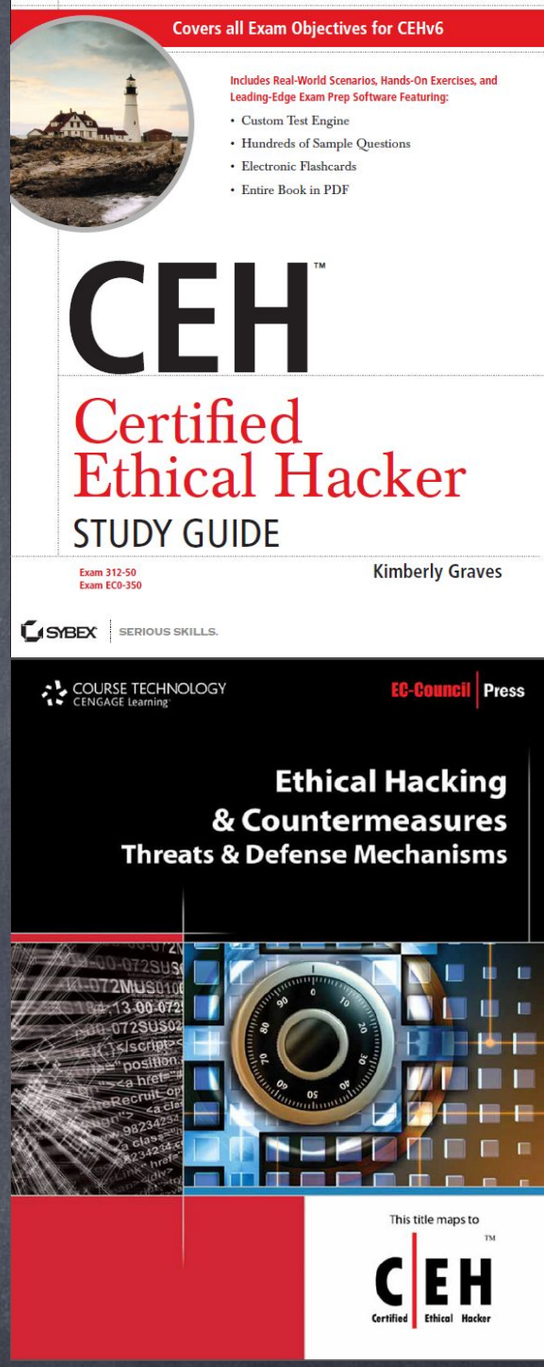
- Разработка и исследование криптографических методов ЗИ в компьютерных системах и сетях

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

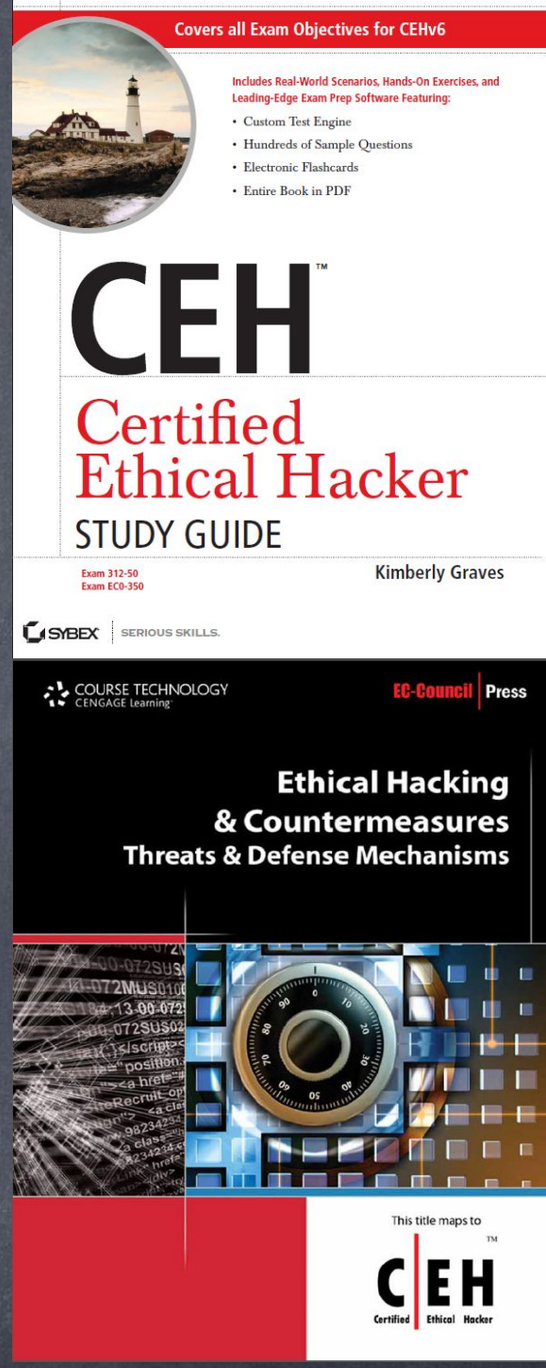
Защищенные компьютерные технологии

- 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)

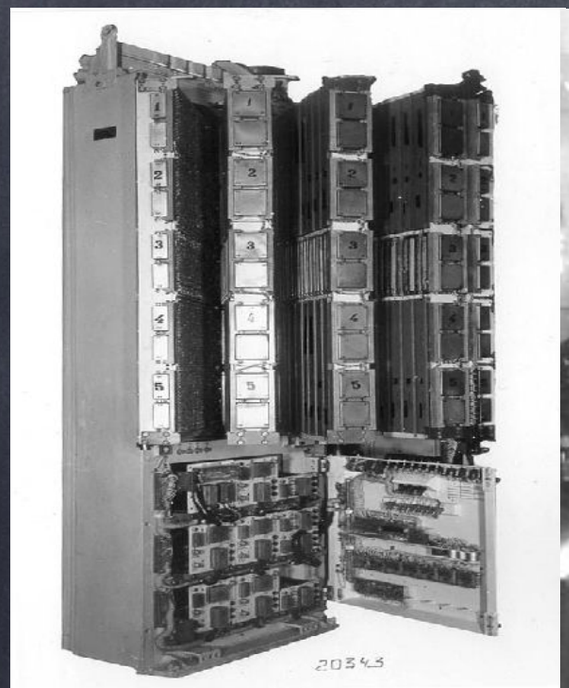


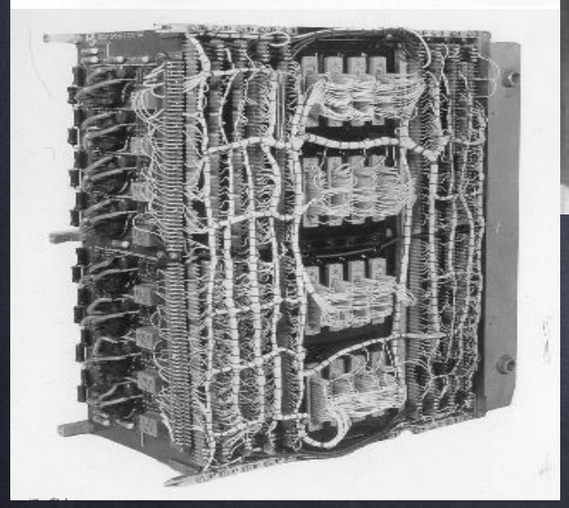
Защищенные компьютерные технологии

- 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 !

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

Особенности криптографии как науки

Криптография как математическая наука

vs

Криптография как инженерная дисциплина

Уязвимости реализации КА

Алгоритмические атаки на КА

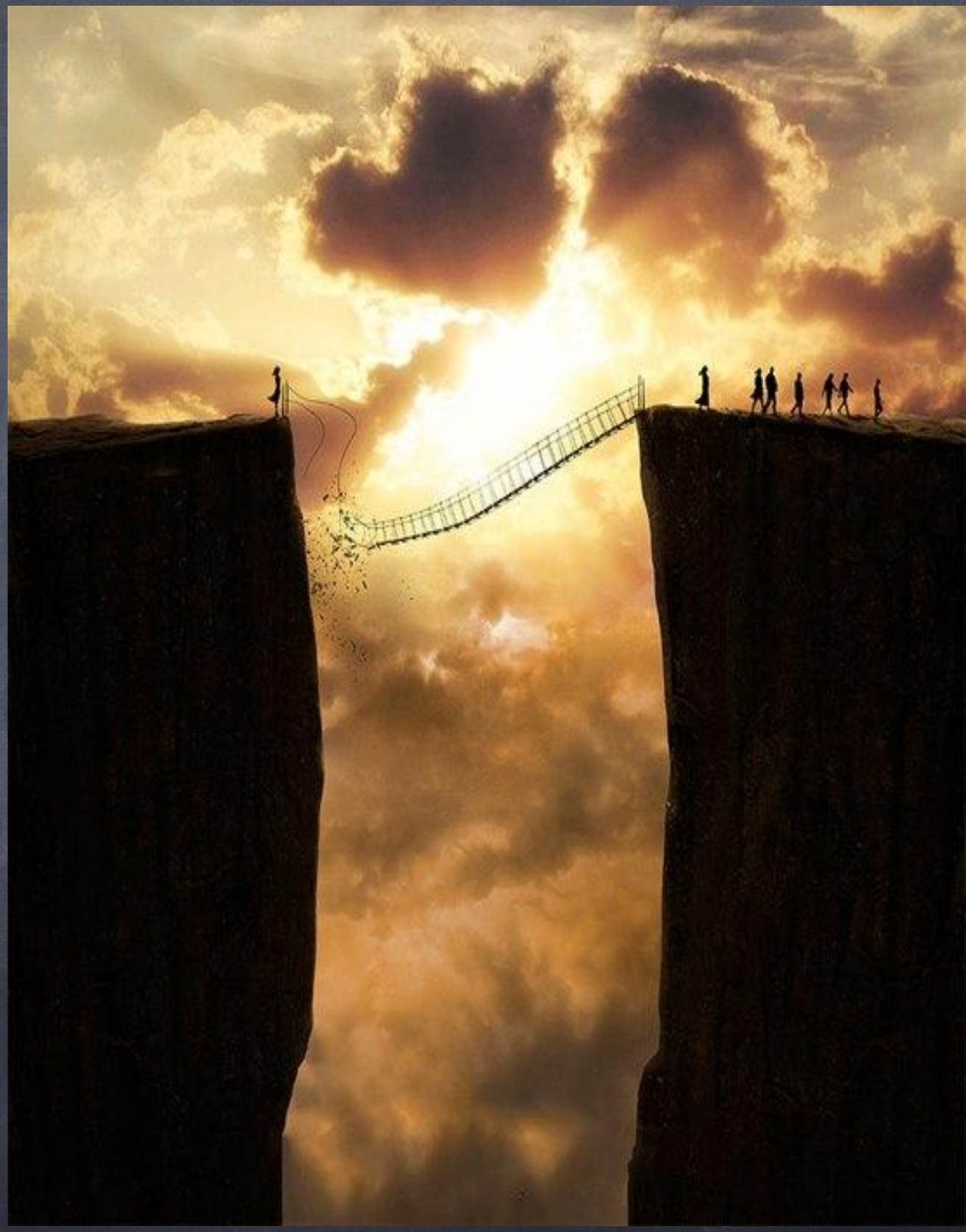
Криптографические бэкдоры

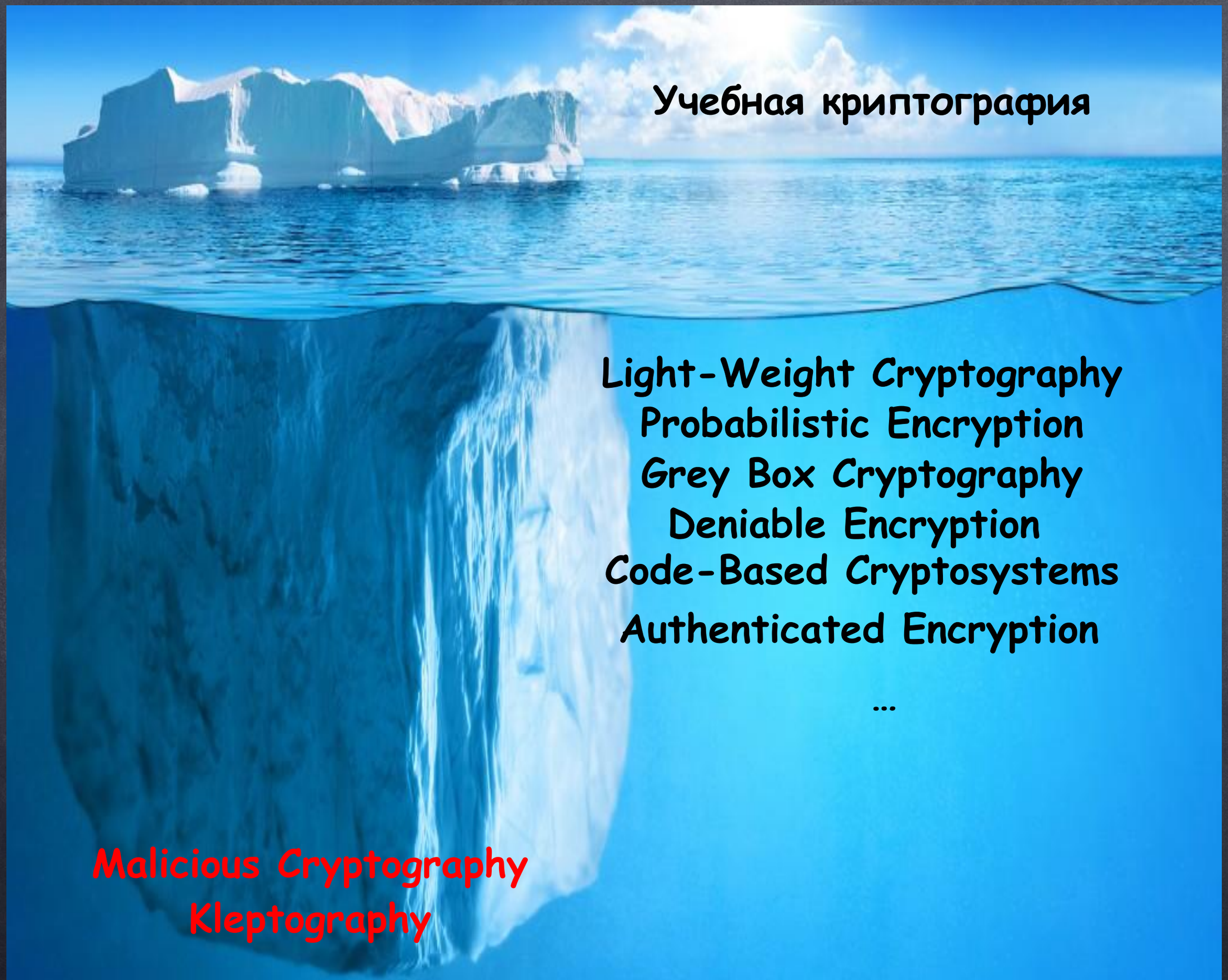
Криптографические скрытые каналы

Криптография
как математическая наука

VS

Криптография
как инженерная наука




Учебная криптография
Light-Weight Cryptography
Probabilistic Encryption
Grey Box Cryptography
Deniable Encryption
Code-Based Cryptosystems
Authenticated Encryption
...
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

1948 г.
К. Шеннон
Теория связи
в секретных системах

- Хеш-функции (ХФ)

- Генераторы псевдослучайных чисел (ГПСЧ)



ГПСЧ – основа стохастических методов защиты информации !

Современная криптография:
криптографические механизмы защиты информации

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

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

- Схемы гибридного шифрования
- Протоколы выработки общего секретного ключа
- Протоколы электронной подписи (ЭП): классическая ЭП, групповая 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

Криптография. История первая

Энигма

А. Тьюринг

1912 - 1954

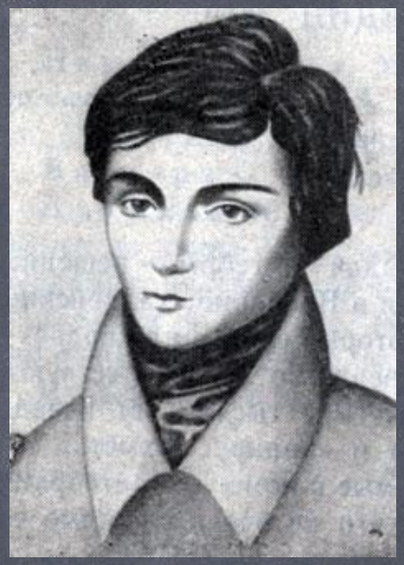
Bombe

Криптография. История первая

Энигма

А. Тьюринг
1912 - 1954

Ф. Бэкон
1561-1626



Э. Галуа
1811-1832

Р. Ривест

Bombe

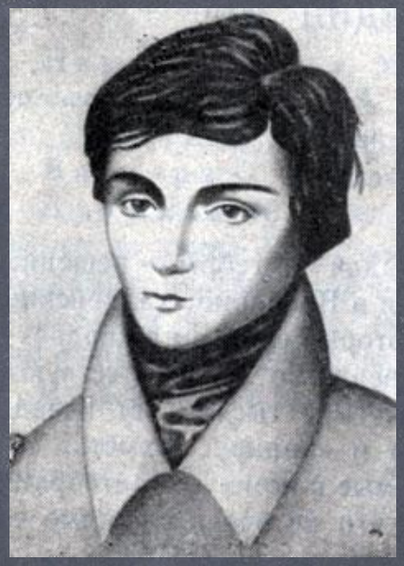
Криптография. История первая

Энигма

А. Тьюринг
1912 - 1954

Bombe

Ф. Бэкон
1561-1626



Э. Галуа
1811-1832

Р. Ривест

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 (2016 г.)

Криптография. История вторая. Государственные стандарты

- США: DES (1974 г.) → AES (2001 г.)
- Россия:
  ГОСТ 28147-89 → Кузнечик (2016 г.)
- Япония:
  FEAL → FEAL-2 → … →FEAL-8
- Китай:
  SM4 (2006 г.)

Криптография. История третья. Теория конечных полей (полей Галуа)

Эварист Галуа

1811-1832

- Теория чисел
- Высшая алгебра
  →Теория полей Галуа
- Высшая геометрия
  →Эллиптические кривые
- Теория сложности вычислений

Криптография. История четвертая. Шифр Ф. Бэкона. Режим 1

Символы алфавита	Ключевая информация			
	Двухлитерный 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*
Z	*babaa*	*b*	*a*	*b*

Криптография. История четвертая.

Символы алфавита	Ключевая информация			
	Двухлитерный 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*
Z	*babaa*	*b*	*a*	*b*

Ф. Бэкон
1561-1626

m = CAT

Зашифрование

1-й шаг: *c* = *bbabb abbbb baabb*

2-й шаг: *c* = **NOCVW ARTVZ PFGVY**

Криптография. История четвертая.

Символы алфавита	Ключевая информация			
	Двухлитерный 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
Z	babaa	b	a	b

Ф. Бэкон
1561-1626

m = CAT

Зашифрование
1-й шаг: c = bbabb abbbb baabb
2-й шаг: c = NOCVW ARTVZ PFGVY

Расшифрование 1
1-й шаг: m = bbabb abbbb baabb
2-й шаг: m = CAT

Криптография. История четвертая.

Символы алфавита	Ключевая информация			
	Двухлитерный 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
Z	babaa	b	a	b

Ф. Бэкон
1561-1626

m = CAT

Зашифрование
1-й шаг: c = bbabb abbbb baabb
2-й шаг: **c = NOCVW ARTVZ PFGVY**

Расшифрование 1
1-й шаг: m = bbabb abbbb baabb
2-й шаг: **m = CAT**

Расшифрование 2
1-й шаг: m´ = abbab baaaa aabab
2-й шаг: **m´ = DOG**

Криптография. История четвертая.

Символы алфавита	Ключевая информация			
	Двухлитерный 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
Z	babaa	b	a	b

Ф. Бэкон
1561-1626

m = CAT

Зашифрование
1-й шаг: *c = bbabb abbbb baabb*
2-й шаг: **c = NOCVW ARTVZ PFGVY**

Расшифрование 1
1-й шаг: *m = bbabb abbbb baabb*
2-й шаг: **m = CAT**

Расшифрование 2
1-й шаг: *m´ = abbab baaaa aabab*
2-й шаг: **m´ = DOG**

Расшифрование 3
1-й шаг: *m ˝ = bbaaa bbaab aabab*
2-й шаг: **m ˝ = PIG**

Криптография. История четвертая. Шифр Ф. Бэкона. Режим 2

Текст-контейнер

Из вереска напиток забыт давным-давно, а был он слаще меда, пьянее, чем вино …

Секретное сообщение

PASSWORD

bbaaa abbbb aabbb aabbb aaaba baaaa abbba abbab

1) изверескана питокзабытдавным давноа былонслащемедапьянеечемвино …
2) извер ескан апито кзабы тдавн ымдав ноабы лонсл ащеме дапья неече мвино …
3) изВЕР Ескан АПито КЗабы ТДАвН ыМДАВ НоабЫ ЛонСл ащеме дапья …
4) из ВЕРЕска нАПитоК ЗабыТ ДАвНыМ-ДАВНо, а бЫЛ он Слаще меда, пьянее …

Символы алфавита	Ключевая информация	
	Двухлитерный код	
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	
Z	babaa	

Криптография. История пятая.

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

Источники информации на русском языке

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) Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире.
– Питер, 2005.
5) Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ.
– М.: Издательский дом «Вильямс», 2005.
6) http://www.enlight.ru/crypto/ (А. Винокуров)
7) Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – Горячая линия «Телеком», 2012.
8) Рябко Б.Я., Фионов А.Н. Криптография в информационном мире. - Горячая линия «Телеком», 2018.
8) Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. - Горячая линия «Телеком», 2010.
9) Иванов М.А. Основы криптографии. В 2-х частях. – М.: Изд-во ГУУ, 2023.

Источники информации на английском языке

1) Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography. 2015. crypto.stanford.edu/~dabo/cryptobook/

2) Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.

3) Niels Ferguson and Bruce Schneier. Practical Cryptography. - Wiley Publishing, 2003.

4) Bellare-Rogaway lecture notes. http://www.cs.ucdavis.edu/ rogaway/classes/227/spring05/book/main.pdf

5) Goldwasser-Bellare lecture notes. http://www.cs.ucsd.edu/users/mihir/papers/gb.pdf

6) Barak's lecture notes. http://www.cs.princeton.edu/courses/archive/fall05/cos433

7) Eric Filiol. Computer viruses: from theory to applications. - Springer-Verlag 2005.

8) Jon Erickson. Hacking: the art of exploitation. 2nd Edition. - No Starch Press, 2008.

9) Adam Young, Moti Yung. Malicious Cryptography: Exposing Cryptovirology. 2004.

Задания для самостоятельной работы

1) Return-Oriented Programming (ROP).
2) Jump Oriented Programming (JOP).
3) Технология безопасного программирования (Buffer Overflow*, Race Condition*, Integer Overflow*, Heap Overflow, Double Free, …).
4) Moving Target Defense -> Morpheus (патенты США)
5) Control Flow Integrity -> SOFIA (патенты США)
6) Memory Tagging Extension -> CHERI (патенты).
7) Криптографические бэкдоры в асимметричных КС (Knapsack, RSA, …).
8) Криптографические бэкдоры в блокчейне.
9) Криптографические бэкдоры в симметричных КС.
10) SETUP-атаки.
11) PUF.
12) Лабораторный практикум по ЗИ (GF, программные модели PRNG, новые статистические тесты, шифр Бэкона, …)

The questions are welcome !