Криптографические методы защиты информации

Курс лекций для специалистов по компьютерной безопасности

Полезные контакты и ссылки

- Племянников Александр Кимович, доцент кафедры «Информационная безопасность»
  - Лекции, диф. зачет, лабораторные и практические занятия
  - Контакты: *alexplem@mail.ru*, *AKPlemyannikov@etu.ru,*
- Лабораторный практикум:
  - Инструментарий https://www.cryptool.org/en/
  - Методические указания размещены на сайте дисциплины https://vec.etu.ru/moodle/course/view.php?id=8299
  - Помещение 2112-2113, корп. II

Специальные дисциплины учебного плана

IV курс

- Основы информационной безопасности
- **Теоретико-числовые методы** в **криптографии**
- Модели безопасности компьютерных систем
- Технические средства и методы защиты информации
- **Криптографические методы защиты информации**

V курс

- **Криптографические протоколы**
- Организационное и правовое обеспечение ИБ
- **Защита ОС и СУБД**
- **Защита компьютерных сетей и телекоммуникаций**
- **Администрирование защищенных информационных систем**
- Модели нарушения безопасности и вирусология
- **Технология разработки инф. систем в защищенном исполнении**
- Инженерно-техническая защита объектов информатизации

Структура рабочей программы курса

Требования к отчетам по лабораторным работам

- Наименование файла отчета - <группа><ФамилияИО>ЛАБ<номер>
- В печатном виде предъявляется титульная страницы с подписью автора и страницы с ЗАКЛЮЧЕНИЕМ
- Страницы скрепляются степлером или скрепкой
- Содержание отчета согласно заданию на работу на Moodle-сайте дисциплины (приоритетнее) и методическим указаниям
- ЗАКЛЮЧЕНИЕ – это обобщение выводов по каждому разделу отчета
  - Шаблон вывода: «Выполнено «действие» и получено «результат»
  - Количество выводов – столько, сколько разделов

Порядок защиты

- Теоретическая подготовка по соответствующему разделу курса из конспекта лекций
- Открытие отчета на компьютере лаборатории
- Демонстрация выполнения указанного преподавателем задания
- Ответы на практические вопросы по теме соответствующего раздела курса
- График защит – 2 работы в месяц

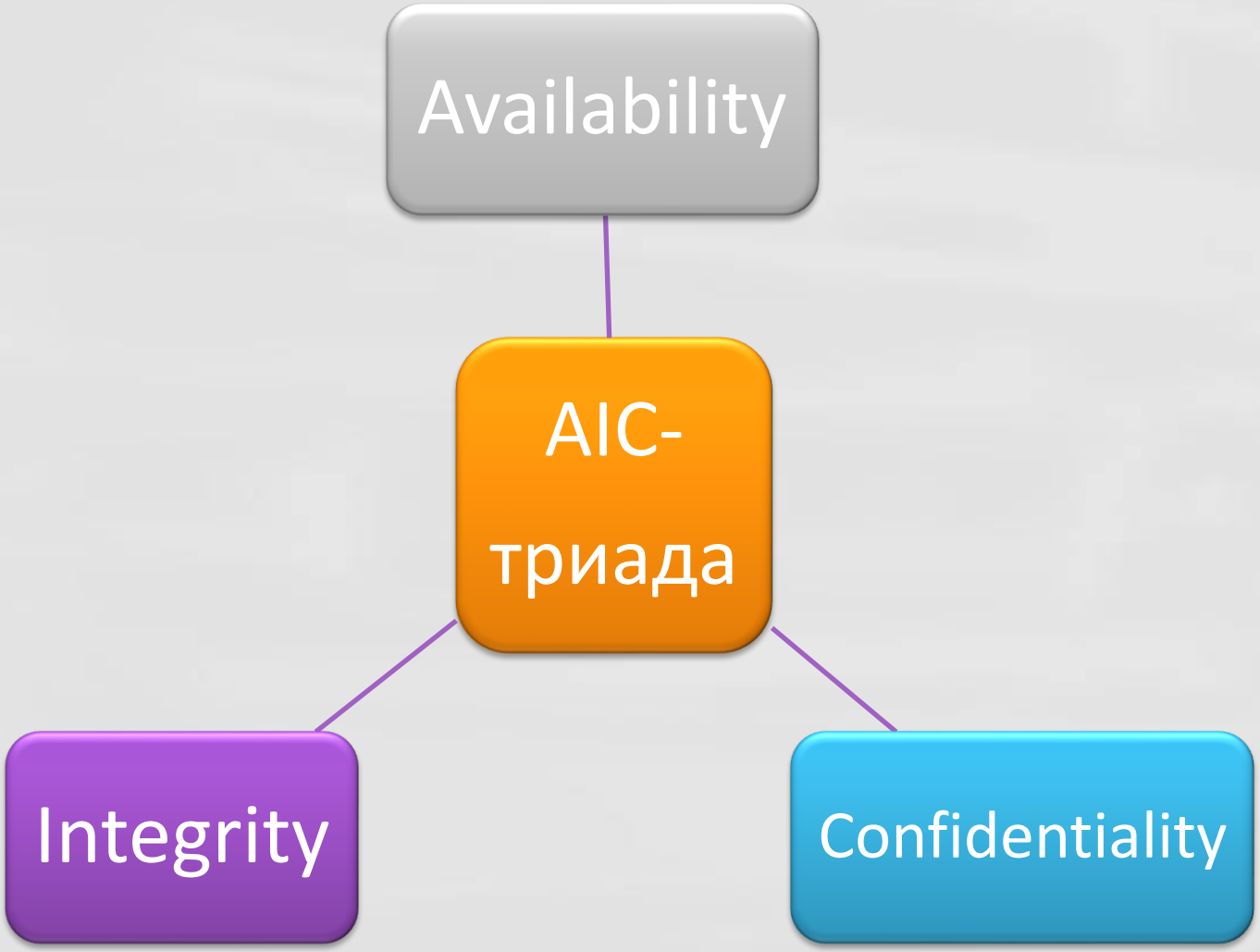
Виды защиты информации по ГОСТ Р 50922-2006

- **Защита информации** – деятельность, направленная на предотвращение защищаемой информации, от несанкционированных и непреднамеренных воздействий :
  - **Правовая защита информации:** защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением
  - **Техническая защита информации:** защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств
  - **Криптографическая защита информации:** защита информации с помощью ее криптографического преобразования
  - **Физическая защита информации:** защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

Место криптографии среди других наук

- Криптография («тайнопись») занимается разработкой методов (криптографических) преобразований информации с целью ее защиты от незаконных пользователей
- Криптоанализ - занимается оценкой сильных и слабых сторон криптографических методов, а также разработкой методов, позволяющих взламывать криптографические преобразования (шифры, например)
- Криптология - наука, занимающаяся исследованиями криптографических преобразований. Криптология состоит из двух частей - криптография и криптоанализ

Цели информационной безопасности



- Доступность
- Целостность
- Конфиденциальность

Угрозы в фокусе криптографии

Задачи криптографии

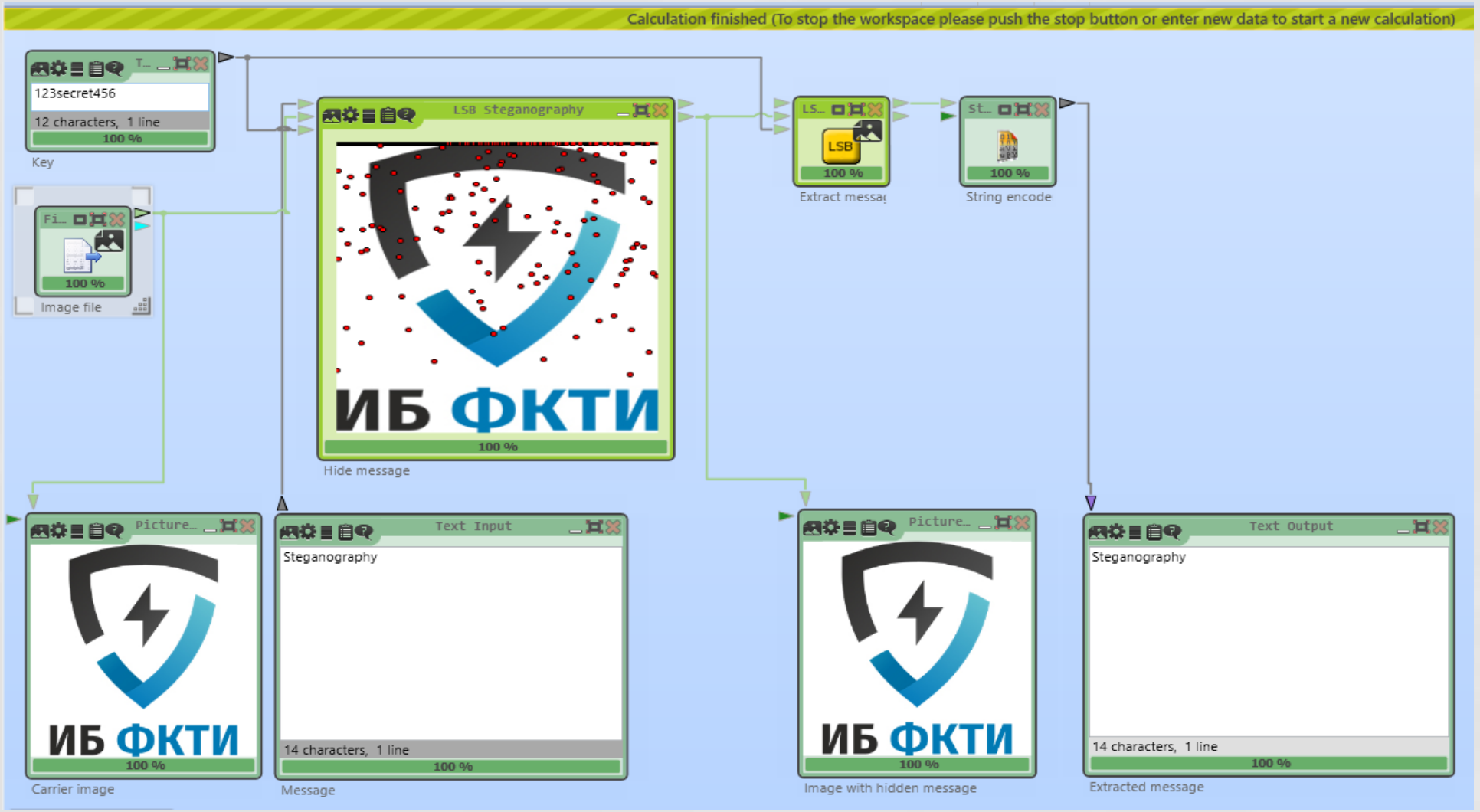
- Обеспечение конфиденциальности - защита содержимого информации от лиц, не имеющих к ней доступа.
- Обеспечение целостности - гарантирование невозможности несанкционированного изменения информации.
- Обеспечение аутентификации – разработка и внедрение методов подтверждения подлинности сторон и самой информации.
- Обеспечение невозможности отказа от авторства - предотвращение возможности отказа субъектов от некоторых совершенных ими действий.

Взаимосвязь идентификации, аутентификации и авторизации

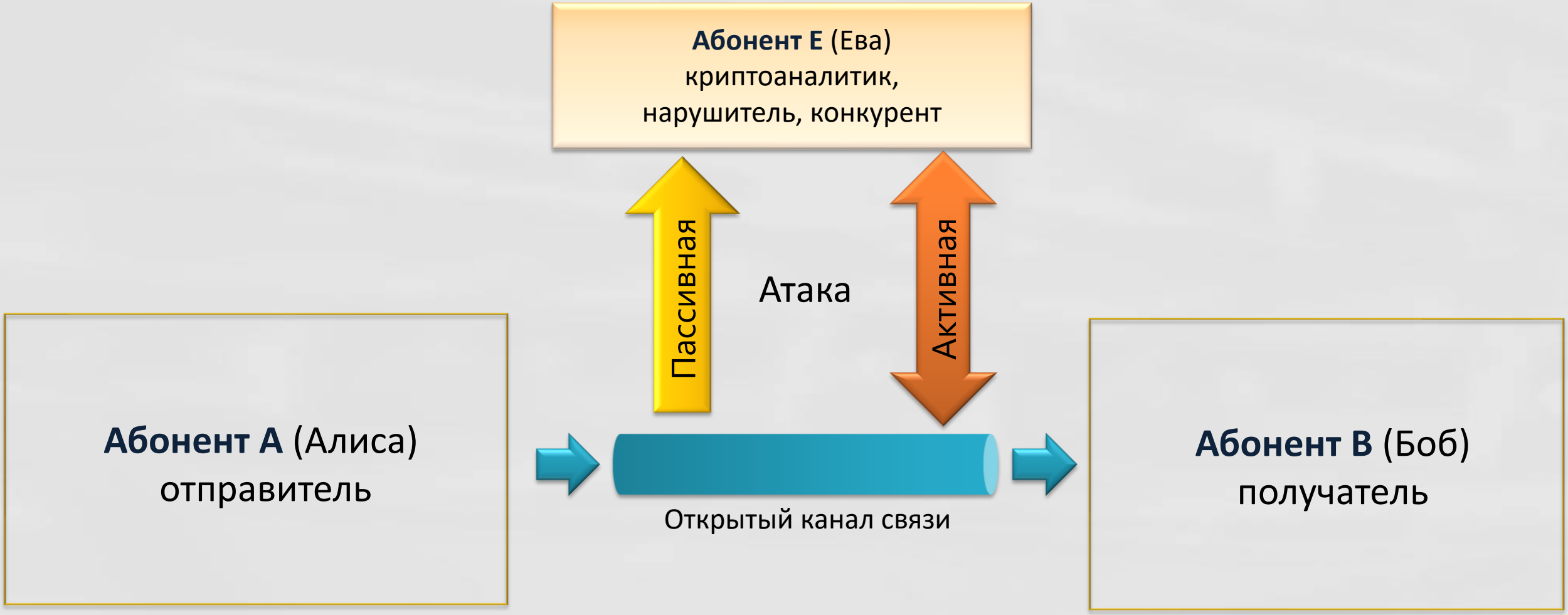
Смежные дисциплины

- Стеганография - наука о скрытой передаче информации путём сохранения в тайне самого факта передачи
- Примеры применения стеганографии:
  - Невидимые чернила (обработка послания реактивом или нагреванием)
  - Скрывающие тексты (кодирование символов сообщения количеством пробелов между словами)
  - Цифровые изображения (метод LSB (Least Significant Bit), кодирование сообщения с помощью самого младшего бита каждого байта)

Демонстрация метода LSB в CrypTool 2



Базовая модель передачи данных



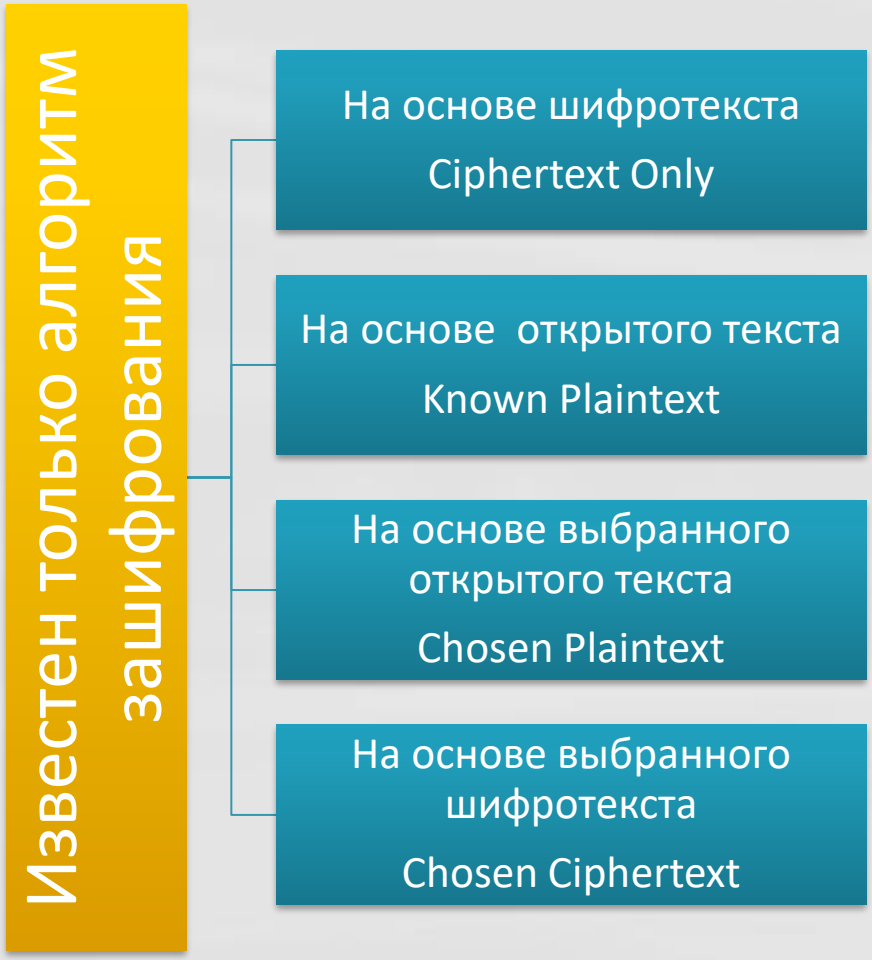
Определения из криптографии

- Открытый текст (***plaintext)***. Данные в читаемом формате, также называемые простым текстом (cleartext).
- Зашифровка (***encipher***). Действие по преобразованию исходных данных в нечитаемый формат.
- Шифротекст (***ciphertext***)- данные в форме, которая выглядит случайной и нечитаемой
- Расшифровка (***decipher***). Действие по преобразованию шифротекста обратно в читаемую форму.
- Шифр (***cipher***) - набор математических правил (алгоритм), используемых для зашифрования и расшифрования.
- Секретный ключ (***secret key***) - секретная информация, используемая при зашифровании/расшифровании сообщений
- Криптосистема (***cryptosystem***)- набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса

Определения из криптоанализа

- Криптоаналитик (нарушитель) - лицо (группа лиц), целью которых является прочтение или подделка защищенных криптографическими методами текстов
  - Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдан потенциальной ценностью информации, которая будет добыта в результате криптоанализа
- Атака (***attack***) -попытки получения какой-либо скрытой информации или скрытой подделкой истиной информации
- Взлом (***cracking***) – успешно проведенная атака

Виды атак



Основной задачей является поиск ключа шифрования или расшифровка данных

Как стать настоящим криптографом ?

Существует только один путь стать хорошим разработчиком криптографических алгоритмов - быть хорошим криптоаналитиком и взламывать алгоритмы. Множество. Снова и снова. Только после того, как обучающийся продемонстрирует способности к криптоанализу чужих алгоритмов, он сможет серьезно браться за разработку собственных алгоритмов.

Брюс Шнайер (Bruce Schneier)

Основные этапы развития криптографии

1. • Интуитивная (до начала XVI века)
2. • Формальная (конец XV века - начало XX века)
3. • Научная (30-е - 60-е годы XX века)
4. • Компьютерная (с 70-х годов XX века)