Курс: **ЭЛЕМЕНТЫ КРИПТОГРАФИЧЕСКОГО АНАЛИЗА**

Кафедра информационной безопасности

Лекция 1 (установочная)

Лектор: Тимонина Елена Евгеньевна,
д.т.н., профессор

E-mail: eltimon@yandex.ru

Слайд 1.1.

1. Общие данные:

- курс рассчитан на один семестр;
- по результатам изучения курса проводится экзамен;
- курс представлен слайдами и комментариями к ним;
- студент сам выбирает время знакомства с материалами курса.

2. Во многие лекции будут включены вопросы и задачи.

Решение задач и ответы на вопросы (в формате word, pdf) следует посылать по электронной почте.

3. В течение семестра будет проведено 4 контрольных работы. Варианты контрольных работ, рекомендации к ним и сроки сдачи будут переданы старостам групп. Работы также должны быть оформлены в word, pdf.

Слайд 1.2.

Для понимания курса необходимо знание:

- математического анализа;
- общей алгебры;
- дискретной математики;
- теории вероятностей и математической статистики.

Слайд 1.3.

Лекции будут выкладываться на Яндекс Диск по ссылке:
https://yadi.sk/d/BgXN-XJzQ_QJOg
и будут доступны всем студентам.

Обращение к диску и папке:

- через любой браузер студенты могут получить доступ к лекциям, сохраненным в папке. Лекции в формате Microsoft PowerPoint будут предоставлены в виде видеофайла со слайдами и комментариями лектора.

Алгоритм скачивания:

- открыть ссылку в браузере
- выбрать нужную лекцию
- нажать сверху в появившемся меню «Скачать» или «Сохранить на Яндекс.Диск, если вы уже зарегистрированы на сервисе.

Алгоритм просмотра и прослушивания:

- Лекции можно открыть с помощью стандартного видеопроигрывателя ОС Windows, а также на смартфонах и планшетах.

Слайд 1.4.

Общение с лектором осуществляется по электронной почте.

Вопросы по курсу и ответы на них преподавателя также передаются по электронной почте.

Ответы могут быть трех типов:

- найти ответ в рекомендованной литературе;
- конкретный ответ на конкретный вопрос;
- преподаватель не понял вопрос, заданный студентом.

Ответ третьего типа, пока студент не сформулировал корректно и полно вопрос по существу курса.

Слайд 1.5.

1. Программа курса и вопросы к экзамену будут выложены в конце семестра.

2. Консультации будут проводиться индивидуально по электронной почте.

3. Итоговая оценка будет складываться из оценки, полученной в течение курса (оцениваться будут ответы на вопросы, решение задач, контрольные работы), и оценки, полученной в результате экзамена. Экзамен будет проводиться в письменной форме и содержать теоретический вопрос и задачу по материалам курса.

4. Студенты, правильно решившие в течение курса все задачи, правильно ответившие на все вопросы лекций, а также успешно выполнившие, правильно и полно оформившие промежуточные контрольные работы, могут рассчитывать на «автомат».

Слайд 1.6.

Обязательная литература

1. Учебное пособие (имеется в библиотеке ВМиК): Теоретические основы информационной безопасности / Грушо А.А., Тимонина Е.Е., Применко Э.А., 2009 г.
2. Б. А. Погорелов, В. Н. Сачков. Словарь криптографических терминов. – М.: МЦНМО, 2006.

Дополнительная литература будет приводится по ходу курса лекций.

Слайд 1.7. Задачи криптографии

Криптография [cryptography] – область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с разработкой *криптографических средств* защиты информации от *угроз* со стороны *противника* и/или *нарушителя,* а также анализом и обоснованием их *криптографической стойкости.*

В настоящее время основными задачами криптографии являются обеспечение:

(1) конфиденциальности,

(2) целостности,

(3) аутентификации,

(4) невозможности отказа,

(5) неотслеживаемости.

Слайд 1.8. Основные понятия (см. Словарь)

1. **Конфиденциальность** (информации) [privacy, confidentiality] – означает, что информация предназначена только определенному кругу лиц и должна храниться в тайне от всех остальных.
2. **Целостность** [integrity] – отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью.
3. **Аутентификация** [authentication] – установление (то есть проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: содержания и источника передаваемых сообщений, сеанса связи, времени взаимодействия и т. д.
4. **Невозможность отказа** [non repudiation] (неотказуемость) – свойство криптографического протокола, состоящее в том, что его участники (все или некоторые) не могут отказаться от факта совершения определенных действий.
5. **Неотслеживаемость** [untracebility] – свойство, означающее невозможность получения противником и/или нарушителем сведений о действиях участников (протокола).

Слайд 1.9. Цель криптографии

Фундаментальная цель криптографии состоит в том, чтобы соответственно обратиться к этим областям и в теории, и в практике.

Цель криптографии – предотвращение и обнаружение обмана и других злонамеренных действий.

Криптография, с некоторой долей условности, делится на: криптосинтез и криптоанализ.

Анализ криптографический [cryptanalysis, криптоанализ] – исследование криптографической системы с целью получения обоснованных оценок ее криптографической стойкости.

Синтез криптографический [cryptosynthesis, криптосинтез] – условно выделяемая часть криптографии (криптологии), связанная с разработкой криптографических (систем криптографических протоколов).

Криптология (математическая криптография) [cryptology (mathematical cryptography)] – отрасль криптографии, математики и математической кибернетики, изучающая математические модели криптографических систем.

Слайд 1.10. Основные понятия

Шифрование [encryption, enciphering] – термин, объединяющий термины зашифрование и расшифрование.

Зашифрование [encryption, enciphering] – процесс преобразования открытого сообщения, в шифрованное сообщение с помощью инъективной функции, зависящей от ключа из ключевого множества.

Расшифрование [decryption, deciphering] – процесс, обратный к зашифрованию, реализуемый при известном значении ключа.

Дешифрование [decryption, breaking of cryptosystem] – процесс аналитического раскрытия противником и/или нарушителем сообщения, открытого без предварительного полного знания всех элементов системы криптографической. Если этот процесс поддается математической формализации, говорят об алгоритме дешифрования.

Атака на криптосистему [attack on the cryptosystem] — попытка противника и/или нарушителя понизить уровень безопасности конкретной системы криптографической на основе определенных методов криптоанализа и при некоторых предположениях криптоанализа.

Обратите внимание (!) на понятия расшифрование и дешифрование: в англоязычной литературе различаются по контексту, в нашей – строгое разграничение понятий. Неправильное использование понятий = снижение оценки!

Слайд 1.11. История

Ниже приведены книги по истории (кому интересно). Их можно скачать в интернете. В интернете есть большое количество книг на эту тему.

1. Соболева Т.А. История шифровального дела в России. – Издательский дом: «ОЛМА–ПРЕСС», 2002.
2. David Kahn, The Codebreakers. The Story of secret writing, New York, Macmillan publishing, 1967.