Темы докладов «Основы информационной безопасности»

В приложении примерный список тем. **Можно брать свои темы**, главное чтобы их содержание имело отношение к информационной безопасности. Совсем хорошо, если будут рассматривать новые и перспективные технологии.

Обычно на 1 лекцию не более двух, максимум трех докладов. Материал не зачитывается с листочка или смартфона, а излагается самостоятельно.

1. **Белорусская криптография**. Основные национальные криптоалгоритмы (симметричные, ассиметричные, хэш, эцп). Где и зачем применяются? В каких продуктах использованы. Сравнение с зарубежными.

2. **Блокчейн**. Криптовалюта (основные виды), как «генерируются», траты на вычисления (энергия), угрозы и уязвимости (платформы, криптобиржи и тд.).

3. **Внедрение SQL-кода,** Межсайтовый скриптинг (XSS). Рассказать про данные уязвимости. Статистика (сколько было утечек\атак, какие сайты подвержены наиболее всего). Объяснить понятными словами с наглядными примерами. Основные механизмы защиты.

4. **Социальная инженерия**. Сущность методов, основные виды, статистика по инцидентам, судебная практика по таким делам.

5. **DDoS-атаки**. Сущность. Несколько основных современных видов реализаций. Способы защиты.

6. **Биометрические методы аутентификации** пользователя.
Биометрические паспорта. Достоинства и недостатки. Сравнение законодательств разных стран в области использования биометрических данных. Уязвимости систем биометрической аутентификации.

7. **GDPR**. Защита персональных данных. Особенности законодательства РФ, РБ, ЕС. Примеры крупных утечек. Практика применения закона о персональных данных.

8. **Пентесты**. Тестирование на проникновение. Суть тестирования, юридические аспекты пентестов. Короткий обзор 3 лучших дистрибутивов для

пентестов (какие утилиты чаще всего используются и для чего). Набор необходимого оборудования для проведения пентестов.
9. **Анализ рисков**. Суть методики, примеры расчета, «лучшие практики».

10. Проблемы информационной безопасности в «**умных домах**». Стандарты шифрования, алгоритмы, протоколы.

11. **Современные алгоритмы шифрования**. На выбор рассмотреть один из современных алгоритмов шифрования (непосредственно шифрования, хэширования или обмена ключами). Область применения. В идеале, показать код программной реализации.

12. **Методы социальной инженерии**. Рассмотреть проблему на примере социальных сетей. Известные случаи мошенничества. Безопасное использование социальных сетей.

13. **Безопасность виртуальных сред**. Угрозы/ уязвимости контейниризированных приложений и облачных сервисов

14. **Концепция AAA** (Authentication, Authorization, Accounting). Протоколы DIAMETR, RADIUS и TACACS+. Область применения, различия, примеры, где используется.

15. **Диффи-Хелман**. Протоколы обмена ключами.

16. Шифрование на **эллиптических кривых**. Основные определения, алгоритмы. Пример Curve 25519

17. Протокол **Диффи — Хеллмана на эллиптических кривых** (ECDHE)

18. **SIEM системы** (Security information and event management). Назначение, примеры, особенности, область применения.

19. Современные системы **видеонаблюдения**. **Видеоаналитика**.

20. **DLP системы** (Data Leak Prevention). Назначение, примеры, особенности, область применения.