



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Б1.В.05 АНАЛИЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)

ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности

Знать:

ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем

Уметь:

ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем

Владеть:

ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

Знать:

ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения

Уметь:

ПК-2.2/Ум1 анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

Владеть:

ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня

защищенности и доверия в компьютерных системах

Знать:

ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности

Уметь:

ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

Владеть:

ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности

ПК-2.3/Нв2 навыками анализа журналов событий и других источников информации о состоянии компьютерной системы

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)	Повышенный	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем Уметь: ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем Владеть: ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения Уметь: ПК-2.2/Ум1 анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Владеть: ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности Уметь: ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

	Владеть: ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности ПК-2.3/Нв2 навыками анализа журналов событий и других источников информации о состоянии компьютерной системы
Базовый	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем Уметь: ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения Уметь: ПК-2.2/Ум1 анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности Уметь: ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

	Пороговый ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности
--	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

	ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Ум1 анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности ПК-2.3/Нв2 навыками анализа журналов событий и других источников информации о состоянии компьютерной системы
Хорошо	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Ум1 анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах
Удовлетворительно	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения

	ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/3н1 методы и инструменты оценки уровня защищенности
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Нормативное регулирование в области анализа безопасности компьютерных систем	ПК-2.1		Экзамен
2	Методы и инструменты проведения анализа безопасности компьютерных систем	ПК-2.2		Экзамен
3	Сбор информации об объекте анализа	ПК-2.3		Экзамен
4	Особенности анализа безопасности СУБД	ПК-2.2 ПК-2.3		Экзамен
5	Особенности анализа безопасности телекоммуникационного оборудования	ПК-2.1 ПК-2.2 ПК-2.3		Экзамен
6	Особенности анализа защищенности беспроводных сетей	ПК-2.1 ПК-2.2 ПК-2.3		Экзамен
7	Анализ безопасности мобильных приложений	ПК-2.1 ПК-2.2 ПК-2.3	Тестирование	Экзамен

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 1 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

6. Оценочные материалы текущего контроля

Раздел 7. Анализ безопасности мобильных приложений

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Тема 7.1. Особенности архитектуры ОС Android. Первичный анализ мобильных приложений ОС Android.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие существуют основные классы атак? Выберите несколько из 4 вариантов ответа:

1. Локальная атака
2. Удаленная атака
3. Атака на поток данных
4. Распределенная атака

2. ... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности.

1. Реагирование на инциденты
2. Управление конфигурацией
3. Управление пользователями

4. Управление рисками

5. Обеспечение устойчивости

3. ... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает. Выберите один из 5 вариантов ответа:

1. Локальная атака
2. Удаленная атака
3. Атака на поток данных
4. Рейдерская атака
5. Социальная инженерия

4. ... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами. Выберите один из 5 вариантов

1. Локальная атака
2. Удаленная атака
3. Атака на поток данных
4. Рейдерская атака
5. Социальная инженерия

5. ... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

6. ... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

7. ... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах. Выберите один из 5 вариантов ответа:

1. Хакер
2. Кракер
3. Фрикер
4. Джокер
5. Анонимайзер

8. К методам защиты от НСД относятся:

1. Разделение доступа
2. Разграничение доступа
3. Увеличение доступа
4. Ограничение доступа
5. Аутентификация и идентификация

9. Выделите группы, на которые делятся средства защиты информации:

1. Физические, аппаратные, программные, криптографические, комбинированные
2. Химические, аппаратные, программные, криптографические, комбинированные
3. Физические, аппаратные, программные, этнографические, комбинированные

10. Что такое компьютерный вирус?

1. Разновидность программ, которые способны к размножению
2. Разновидность программ, которые самоуничтожаются

3. Разновидность программ, которые не работают
4. Разновидность программ, которые плохо работают

11. Как подразделяются вирусы в зависимости от деструктивных возможностей?:

1. Сетевые, файловые, загрузочные, комбинированные
2. Безвредные, неопасные, опасные, очень опасные
3. Резидентные, нерезидентные
4. Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "черви", компаньон-вирусы

12. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется:

1. Политикой информации
2. Защитой информации
3. Политикой безопасности
4. Организацией безопасности

13. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:

1. Системой угроз
2. Системой защиты
3. Системой безопасности
4. Системой уничтожения

14. Какие атаки предпринимают хакеры на программном уровне?

1. Атаки на уровне ОС
2. Атаки на уровне сетевого ПО
3. Атаки на уровне пакетов прикладных программ
4. Атаки на уровне СУБД

15. Что такое криптография?

1. Метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2. Область доступной информации
3. Область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

16. Какими методами можно оценить защищенность компьютерной системы?

1. Пентестирование
2. Анализ рисков
3. Опрос пользователей
4. Все вышеперечисленные методы

17. Какие виды уязвимостей могут быть обнаружены при пентестировании компьютерной системы?

1. Уязвимости в конфигурации
2. Уязвимости в коде программного обеспечения
3. Уязвимости в сетевых протоколах
4. Все вышеперечисленные виды уязвимостей

18. Какие виды атак могут использоваться для компрометации компьютерной системы?

1. Phishing
2. Brute-force атаки
3. DoS/DDoS атаки
4. Все вышеперечисленные виды атак

19. Между какими уровнями работает протокол SSL?

1. Канальным и физическим
2. Сетевым и канальным
3. Транспортным и сетевым

4. Прикладным и транспортным

20. Какие из следующих популярных VPN-протоколов работают на сетевом уровне модели ISO/OSI?

1. OpenVPN
2. PPTP
3. IPSEC
4. L2TP

21. МЭ уровня приложения создает:

1. Виртуальное соединение между клиентом и сервером
2. Туннель между клиентом и сервером
3. Временное соединение между клиентом и сервером
4. Реальное соединение между клиентом и сервером

22. Какое средство необходимо использовать для определения того, уязвим ли хост к известным атакам?

1. Honey Pot
2. Padded Cell
3. Сканер безопасности

23. Что из указанного ниже является активными сетевыми атаками?

1. Анализ данных межсетевого информационного обмена
2. Пассивный перехват
3. Спуфинг
4. Подглядывание за вводом пользователя

24. Какой вид атаки на WiFi-сети направлен на получение доступа к данным, передаваемым между устройствами и точкой доступа?

1. Атака Man-in-the-Middle
2. Атака Replay Attack
3. Атака Rogue Access Point
4. Атака Denial-of-Service (DoS)

25. Какая из этих угроз безопасности СУБД связана с неправильной конфигурацией доступа?

1. SQL Injection
2. Buffer Overflow
3. Denial of Service (DoS)
4. Утечка данных (Data Leakage)

26. Сканирование сетевых портов помогает определить:

1. Установленное программное обеспечение
2. Версию операционной системы
3. Запущенные сетевые сервисы
4. Все из перечисленного

27. Программное обеспечение Wireshark чаще всего применяется для:

1. Перехвата и анализа сетевого трафика
2. Подбора паролей
3. Проведения фаззинг-тестирования
4. Для организации vpn-соединения

28. Что означает аббревиатура VPN?

1. Virtual Private Network
2. Virus Protection Network
3. Visual Private Network
4. Virtual Protection Network

29. К сетевым сканерам относятся:

1. Nmap
2. John the Ripper

3. Honey Pot

4. Ни одно из перечисленных средств

30. Что из перечисленного является примером межсайтового скриптинга (XSS)?

1. Изменение содержимого веб-страницы

2. Взлом сервера базы данных

3. Подмена запросов

4. Удаленное управление компьютером пользователя

7. Оценочные материалы промежуточной аттестации

1 семестр, Экзамен

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Вопросы/Задания:

1. Какая проблема возникает при использовании асимметричной криптографии?

2. В чём заключается суть атаки «человек посередине» при обмене открытыми ключами?

3. Какие уязвимости обычно устраняются путём установки обновлений ("патчей")?

4. Как может быть выполнено отслеживание маршрута при ограничении прохождения трафика UDP и ICMP?

5. Какие методы выявления уязвимостей применяются в локальных сканерах (устанавливаемых в виде агентов)?

6. Какие ограничения имеются при использовании ARP Ping для идентификации сетевых объектов?

7. Проверки какого типа требуют дополнительной верификации наличия уязвимости?

8. Какие предположение относительно операционной системы удалённого узла можно сделать, основываясь на том, что на узле открыты порты 3389/tcp, 135/tcp, 445/tcp?

9. Какие из вариантов аутентификации EAP уязвимы к атакам по словарю?

10. Какие из вариантов аутентификации EAP предполагают аутентификацию клиента на основе сертификата?

11. В каком случае атака SSL Strip окажется неуспешной?

12. От имени какой учётной записи запускается поток, обслуживающий запрос к web-приложению с анонимным доступом?

13. Какая техника может быть использована для фиксации идентификатора сессии при атаке на клиента web-приложения?

14. Каким образом можно использовать внедрение SQL кода для просмотра произвольных таблиц на сервере SQL?

15. С помощью какой уязвимости можно получить доступ к содержимому сценария на web-сервере?

16. Как может быть получен список файлов на web-сервере, помимо использования уязвимости «Индексирование директорий»?

17. Какой вариант XSS-атаки требует перехода по ссылке, сформированной злоумышленником?

18. На чём основан децентрализованный вариант управления бот-сетями?

19. При использовании DNS-туннелирования нуждается ли клиентская часть в прямом доступе к серверной части?

20. На чём основано использование протоколов прикладного уровня для создания скрытых каналов взаимодействия?

21. В чём заключается главный недостаток использования заголовков сетевого и транспортного уровней для создания скрытых каналов взаимодействия?

22. Что такое Exploit Kit?

23. Что такое landing page (целевая страница) в составе Exploit Kit?

24. По какой части идентификатора пользователя Windows (SID) можно выделить учётную запись локального администратора?

25. Как можно быстро перечислить сайты, расположенные на одном адресе?

26. Как работает технология VMBR (Virtual Machine Based Rootkit)?

27. Как можно использовать неавторизованный сервер DHCP для атак «человек посередине»?

28. На истощение какого ресурса чаще всего направлена атака UDP Flood?

29. Какие угрозы связаны с использованием протокола DHCP?

30. В каком случае более точно перечислены типы проверок, используемых в сетевых сканерах безопасности?

31. В каком случае наиболее правильно перечислены "векторы атак" на сервис DNS?

32. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?

33. Можно ли использовать ARP-запрос для добавления записи в ARP-таблицу?

34. Какие алгоритмы используются для обеспечения целостности передаваемых данных?

35. Как может быть использовано нарушителем сообщение "ICMP Redirect"?
36. К какому шагу цикла PDCA (Plan, Do, Check, Act) относится тестирование на проникновение?
37. Какой из методов идентификации узлов сети работает только в пределах только одного сетевого сегмента?
38. В каком из методов идентификации узлов сети вывод об обнаружении узла основывается на получении в ответ ICMP сообщения об ошибке?
39. Какой из методов сканирования портов позволяет определить факт фильтрации порта TCP?
40. Какие типы проверок используются в сетевых сканерах безопасности?
41. В каком случае более точно названы типы агентов сканирования, используемых в современных системах управления уязвимостями?
42. Что лежит в основе технологии «Domain flux», использующейся для управления бот-сетями?
43. Как можно избежать появления сообщения о конфликте IP-адресов при ARPспуфинге с использованием ARP-запроса?
44. Какой SSID указывается во фрейме Probe Request при поиске беспроводных сетей методом активного сканирования?
45. Как можно узнать SSID беспроводной сети, настроенной на работу в скрытом режиме?
46. Какое устройство рассылает фреймы Beacon в беспроводных сетях без точки доступа?
47. Какой фрейм можно использовать для принудительного отключения клиента от точки доступа?
48. В каком фрейме передаётся пароль для беспроводной сети с аутентификацией WPA2-PSK?
49. В чём главное отличие ложного сервера RADIUS от штатного, используемого для аутентификации беспроводных клиентов?