Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

ОП.06 Основы информационной безопасности

для специальности

09.02.12 Техническая эксплуатация и сопровождение информационных систем

квалификация: специалист по технической эксплуатации и сопровождению информационных систем

Москва
2026

Фонд оценочных средств учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, утвержденного приказом Минпросвещения РФ от 10 марта 2024 г. № 184 (зарегистрирован в Минюсте РФ 14 апреля 2025 г. N 818449).

Внутренняя экспертиза:
Заведующая УМУ Заметта Д.Н.

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

ОП.06 Основы информационной безопасности

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Тема 1. Введение в информационную безопасность	ОК 02, ЛР 1-21	- выполнение практических заданий; -выполнение самостоятельных работ по темам дисциплины; -тестирование, оценка за промежуточную аттестацию
2	Тема 2**.** Управление безопасностью информации		
3	Тема 3. Криптография		
4	Тема 4**.** Защита сетевой инфраструктуры		
5	Тема 5. Безопасность приложений		
6	Тема 6. Защита данных		
7	Тема 7. Безопасность облачных технологий		
8	Тема 8. Инциденты безопасности		
9	Тема 9. Социальная инженерия и человеческий фактор		
10	Тема 10. Будущее информационной безопасности		

2. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы контроля и оценки результатов обучения
Знания: сущность и понятие информационной безопасности, характеристику ее составляющих;	**«Отлично»** - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные	**Текущий контроль при проведении:**

место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности. **Умения:** классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации	программой учебные задания выполнены, качество их выполнения оценено высоко. **«Хорошо»** - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. **«Удовлетворительно»** - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. **«Неудовлетворительно»** - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	*-письменного/устного опроса;* *-тестирования;* *- выполнения практических работ;* *-оценки результатов самостоятельной работы* **Промежуточная аттестация** *в форме дифференцированного зачета*

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Основные понятия и определения информационной безопасности.
2. История и развитие информационной безопасности.
3. Актуальные угрозы и риски в информационной безопасности
4. Нормативно-правовое регулирование в области ИБ.
5. Политики и процедуры безопасности. Оценка рисков и управление ими.
6. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)
7. Основы криптографии: симметричные и асимметричные алгоритмы.
8. Хэширование и цифровые подписи.
9. Применение криптографии в приложениях.
10. Стеганография.

11. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.)
12. Использование VPN и межсетевых экранов
13. Уязвимости веб-приложений (OWASP Top Ten).
14. Безопасное программирование: лучшие практики.
15. Тестирование на проникновение и анализ уязвимостей.
16. Шифрование данных в покое и в транзите.
17. Резервное копирование и восстановление данных.
18. Управление доступом к данным
19. Особенности безопасности в облачных средах.
20. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности
21. Реакция на инциденты и управление ими.
22. Анализ инцидентов и цифровая криминалистика.
23. Восстановление после инцидента. Кибербезопасность.
24. Промышленный шпионаж.
25. OSINT.
26. Форензика
27. Психология атак: социальная инженерия.
28. Обучение сотрудников информационной безопасности
29. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн).
30. Этические аспекты информационной безопасности.

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т. п.

Критерии оценки устного опроса студентов:

Оценка **«отлично»:**

- глубокое и прочное усвоение материала темы или раздела;
- полные, последовательные, грамотные, логически излагаемые аргументированные ответы;
- демонстрация обучающимся знаний в объеме пройденной программы и дополнительно рекомендованной литературы;
- воспроизведение учебного материала с требуемой степенью точности.

Оценка **«хорошо»:**

- наличие несущественных ошибок, не достаточно аргументированные ответы на вопросы;
- демонстрация обучающимся знаний в объеме пройденной программы;
- четкое изложение учебного материала.

Оценка **«удовлетворительно»:**

- наличие несущественных ошибок в ответе, отсутствие аргументации, но достаточно грамотное и логичное изложение;
- демонстрация обучающимся недостаточно полных знаний по пройденной программе, отсутствие аргументации;
- не структурированное, не грамотное и не логичное изложение учебного материала при ответе.

Оценка **«неудовлетворительно»:**

- незнание материала темы или раздела;
- серьезные ошибки при ответе.

Тестирование

1. Перечислите методы обеспечения информационной безопасности (ИБ).
а) Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
б) Персональная ответственность руководителей, определение состава конфиденциальных сведений, наличие специализированной службы безопасности
в) Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение

2. К каким средствам относятся средства защиты, которые реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи. Эти нормы не являются обязательными, но несоблюдение их ведет обычно к потере авторитета и престижа человека?
а) Морально-этические
б) Организационные
в) Принуждение

3. Назовите главные требования к организации эффективной работы системы защиты информации (СЗИ) фирмы.
а) Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
б) Персональная ответственность руководителей, определение состава конфиденциальных сведений, определение порядка доступа персонала и наличие специализированной службы безопасности
в) Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение
4. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.)?
а) Организационный
б) Препятствие
в) Управление доступом

5. Как называется метод защиты информации регулированием использования всех ресурсов системы (элементов БД, программных и технических средств)?
а) Определение состава конфиденциальных сведений
б) Программно-аппаратный
в) Управление доступом

6. Какие средства предназначены для противодействия средствам технической разведки и формирования рубежей охраны территории и здания с помощью технических средств?
а) Маскировка
б) Организационные
в) Инженерно-технические

7. Как называется метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности НСД к ней сводились бы к минимуму?
а) Принуждение
б) Организационный
в) Регламентация

8. К каким средствам относятся меры управленческого, режимного и технологического характера, побуждающие персонал соблюдать правила СЗИ фирмы?
а) Принуждение
б) Организационные
в) Инженерно-технические

9. Могут ли лица, проектирующие и модернизирующие систему защиты, контролирующие и анализирующие ее работу, быть пользователями этой системы?
а) Не могут быть
б) Могут быть

10. Что является главным элементом любой, даже самой технически совершенной, СЗИ?
а) Подбор, расстановка и обучение персонала
б) Сознательность, обученность и ответственность персонала
в) Пропускной режим на территории, в здании и помещениях фирмы

11. Перечислите средства обеспечения ИБ.
а) Организационные, морально-этические, законодательные, инженерно-технические, программно-аппаратные, криптографические
б) Персональная ответственность руководителей, определение состава конфиденциальных сведений, наличие специализированной службы безопасности
в) Препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение

12. Как называется метод защиты информации регулированием использования всех ресурсов системы (элементов БД, программных и технических средств)?
а) Определение состава конфиденциальных сведений
б) Программно-аппаратный
в) Управление доступом

13. Какие средства предназначены для защиты информации в компьютерах и серверах?
а) Препятствие
б) Организационные
в) Программно-аппаратные

14. Как называется метод защиты информации путем ее криптографического закрытия?
а) Маскировка
б) Программно-аппаратный
в) Криптографический

15. К каким средствам относятся средства, предназначенные для защиты конфиденциальной информации методами криптографии?
а) Маскировка
б) Криптографические
в) Программно-аппаратные

16. Какой организацией разрабатываются и меняются составные части криптографической защиты, коды, пароли и другие ее атрибуты?
а) ГОСТом
б) Инженерно-технической
в) Специализированной

17. Что нужно делать с содержанием составных частей элементов, методов и средств защиты информации в рамках любой системы защиты с целью предотвращения их раскрытия заинтересованным лицом?
а) Регулярно изменять
б) Шифровать
в) Ставить пароли

18. Как называется такой метод защиты, который побуждает пользователя и персонал системы не нарушать сложившиеся моральные и этические нормы (как регламентированные, так и "неписаные")?
а) Принуждение
б) Морально-этический
в) Побуждение

19. Допускается ли применение пользователями собственных систем шифровки?
а) Допускается
б) Не допускается

20. К каким средствам защиты относятся сооружения инженерной защиты (заборы, решетки, стальные двери, кодовые замки, сейфы и др.)?
а) Принуждение
б) Организационные
в) Инженерно-технические

21. Что является угрозой для компьютерной системы (КС)?
а) условия, предоставляющие потенциальную возможность для нанесения ей ущерба
б) внешние электромагнитные наводки
в) работа в автономном режиме

22. Как называются угрозы, направленные на изменение или полное уничтожение информации?
а) Угрозы нарушения целостности
б) Угрозы нарушения работоспособности

в) Угрозы нарушения конфиденциальности информации

23. Как называются угрозы, направленные на снижение работоспособности системы, либо на блокирование доступа к некоторым ресурсам?
а) Угрозы нарушения целостности
б) Угрозы нарушения работоспособности
в) Угрозы нарушения конфиденциальности информации

24. К какому типу угроз относятся угрозы, связанные с целенаправленными действиями нарушителя: служащего, посетителя, конкурента, наемника и т.д?
а) Случайные воздействия
б) Преднамеренные угрозы
в) Угрозы нарушения целостности

25. К какому типу угроз компонентам КС относятся угрозы, связанные с временным прекращением центральным процессором текущей работы для выполнения некоторых посторонних действий, по завершении которых процессор возвращается в прежнее состояние и продолжает прерванную работу?
а) Прерывание
б) Перехват
в) Модификация
г) Подделка (фальсификация)

26. Как называется процесс, в результате которого злоумышленник может добавить некоторый фальшивый процесс в систему для выполнения нужных ему, но не учитываемых системой действий, либо подложные записи в файлы системы или других пользователей?
а) Прерывание
б) Перехват
в) Модификация
г) Подделка (фальсификация)

27. К какому типу относится прерывание, которое инициируются изнутри основной программы при помощи специальных команд процессора?
а) Программное
б) Аппаратное
в) Перехват

28. Что такое закладка?
а) Несанкционированное изменение структуры КС
б) Несанкционированный доступ в КС
в) Несанкционированное изменение программы в КС

29. Что является основной задачей на этапе эксплуатации КС?
а) Исключение ошибок и возможности внедрения закладок

б) Выявление закладок и ошибок, а также обеспечение целостности, неизменности структур
в) Дублирование информации

30. Что является универсальным средством проверки адекватности и работоспособности КС?
а) Дублирование
б) Тестирование
в) Многослойная «фильтрация»

31. Как называются угрозы, направленные на разглашение конфиденциальной или секретной информации, когда информация становится известной лицам, которые не должны иметь к ней доступ?
а) Угрозы нарушения целостности
б) Угрозы нарушения работоспособности
в) Угрозы нарушения конфиденциальности информации

32. К какому типу угроз относятся аварийные ситуации из-за стихийных бедствий и отключений электропитания, отказы и сбои аппаратуры, ошибки в программном обеспечении, ошибки в работе обслуживающего персонала и пользователей, помехи в линиях связи из-за воздействия внешней среды?
а) Случайные воздействия
б) Преднамеренные угрозы
в) Угрозы нарушения целостности

33. Как называется процесс, в результате которого злоумышленник получает доступ к программным средствам и различного рода физическим носителям информации?
а) Прерывание
б) Перехват
в) Модификация
г) Подделка (фальсификация)

34. Как называется процесс, в результате которого злоумышленник получает не только доступ к компонентам (БД, программам, аппаратным элементам) компьютерной системы, но и манипулирует ими (изменяет, видоизменяет)?
а) Прерывание
б) Перехват
в) Модификация
г) Подделка (фальсификация)

35. К какому типу относится прерывание, которое возникает тогда, когда какое-либо устройство нуждается в экстренном обслуживании, и, как правило, такое прерывание - большая неожиданность для центрального процессора?
а) Программное
б) Аппаратное
в) Перехват

36. Как называется процесс получения нарушителем доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности?
а) Перехват
б) Модификация
в) Несанкционированный доступ

37. Что является основной задачей на этапе разработки и при модернизации КС?
а) Исключение ошибок и возможности внедрения закладок
б) Выявление закладок и ошибок, а также обеспечение целостности, неизменности структур
в) Дублирование информации

38. Как называется независимая (возможно разными организациями) разработка одного и того же блока алгоритма программы или устройства КС?
а) Дублирование
б) Тестирование
в) Многослойная «фильтрация»

39. Что предполагает поэтапное выявление ошибок и закладок определенного класса КС?
а) Дублирование
б) Тестирование
в) Многослойная «фильтрация»

40. Как влияет автоматизация процесса разработки на возможности внедрения закладок?
а) Не влияет
б) Существенно снижает
в) Повышает
41. Что является целью аутентификации электронных документов?
а) их защита от возможных видов злоумышленных действий (перехват, маскарад и т.д.)
б) статистическая обработка произвольного или фиксированного текста
в) присвоение субъектам доступа идентификаторов

42. Для чего используется ЭЦП?
а) для статистической обработки произвольного или фиксированного текста
б) для присвоения субъектам доступа идентификаторов
в) для аутентификации текстов, передаваемых по телекоммуникационным каналам

43. В чём состоит основное достоинство ЭЦП?
а) удостоверяет, что подписанный текст исходит от лица, поставившего подпись; не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом; гарантирует целостность подписанного текста
б) удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
в) гарантирует целостность подписанного текста

44. Из каких процедур состоит система ЭЦП?
а) процедура постановки подписи
б) процедура постановки подписи и процедура проверки подписи
в) процедура проверки подписи

45. Какой ключ используется в процедуре постановки подписи?
а) секретный ключ отправителя сообщения
б) открытый ключ отправителя сообщения
в) секретный и открытый ключ отправителя сообщения

46. Какой ключ используется в процедуре проверки подписи?
а) секретный ключ отправителя сообщения
б) открытый ключ отправителя сообщения
в) секретный и открытый ключ отправителя сообщения

47. Какой ключ генерируется для каждого из абонентов, посылающих друг другу подписанные электронные документы?
а) секретный и открытый
б) секретный ключ
в) открытый ключ

48. Позволяет ли открытый ключ вычислить секретный ключ?
а) позволяет
б) не позволяет
в) в зависимости от степени секретности

49. Какую информацию содержит каждая подпись?
а) дату подписи; срок окончания действия ключа данной подписи; собственно цифровую подпись
б) дату подписи; информацию о лице, подписавшем файл; собственно цифровую подпись
в) дату подписи; срок окончания действия ключа данной подписи; информацию о лице, подписавшем файл; идентификатор подписавшего (имя открытого ключа); собственно цифровую подпись

50. Для чего предназначена хэш-функция?
а) для сжатия подписываемого документа M до нескольких десятков или сотен бит
б) для расшифровки секретного ключа
в) для получения открытого ключа отправителя

51. Какие карты являются наименее защищенными от фальсификации?
а) Виганд
б) магнитные
в) смарт-карты

52. Какие карты имеют максимальную защищенность?
а) смарт-карты

б) Виганд
в) штриховые

53. В каких идентификаторах идентификационный признак слабо или совсем не связан с личностью предъявителя?
а) атрибутивных
б) биометрических
в) автоматизированных

54. Какие идентификаторы основаны на использовании индивидуальных биологических особенностей человека?
а) атрибутивные
б) биометрические
в) автоматизированные

55. Что используется для биометрической идентификации человека?
а) пластиковые карты, папиллярные узоры пальцев, узоры сетчатки глаз, форма кисти руки
б) папиллярные узоры пальцев, узоры сетчатки глаз, форма кисти руки, особенности речи, форма и размеры лица, динамика подписи, ритм работы на клавиатуре
в) пластиковые карты, особенности речи, форма и размеры лица, динамика подписи, ритм работы на клавиатуре

56. Как называется метод идентификации, в котором папиллярные узоры считываются с пальца специальным сканером?
а) Дактилоскопический
б) Параметрический
в) Биометрический

57. Какой метод идентификации используется в системах «Кордон» и «Папилон»?
а) Биометрический
б) Параметрический
в) Дактилоскопический

58. Какие методы идентификации пока не нашли широкого применения?
а) по ритму работы на клавиатуре
б) по форме кисти рук
в) по запаху и термическим характеристикам тела

59. В чём заключается достоинство биометрических методов идентификации?
а) они не требуют дополнительных аппаратных затрат
б) очень высокая вероятность обнаружения попыток несанкционированного доступа
в) идентификация проводится с использованием всех признаков

60. На чём основывается идентификация по ритму работы на клавиатуре?
а) на измерении скорости печати

б) на измерении времени между последовательным нажатием двух клавиш
в) на интенсивность нажатия клавиш

***Критерии оценки**:*

- оценка «отлично» выставляется студенту, если набрано 90-100% правильных ответов;
- оценка «хорошо» выставляется студенту, если набрано 71 - 89% правильных ответов;
- оценка «удовлетворительно» выставляется студенту, если набрано 51 - 70% правильных ответов;
- оценка «неудовлетворительно» выставляется студенту, если набрано 0 - 50% правильных ответов.

Практические задания

Задание 1: Зашифровать стихотворение в одной из традиционных криптосистем своего варианта.

Задание 2: Подготовить к отправке сообщение своего варианта с присоединённой ЭЦП, для этого:
a) Зашифровать двоичным кодом текст сообщения своего варианта, используя данные таблицы.
b) Вычислить хэш-функцию.
c) Придумать и записать в тетрадь секретный ключ Кх.
d) Вычислить значение ЭЦП.
e) Записать сообщение М1, для удобства проверки отделять байты пробелом.
f) Вычислить значение открытого ключа отправителя Ку.

Задание 3: Проверьте диск С с помощью антивирусных пакетов и запишите время, затраченное программой на полную проверку диска.
Сравните и запишите в тетрадь количество обнаруженных вирусов и время проверки для разных антивирусных пакетов.
Пролечите флешку с вирусами с помощью любого пакета.

Критерии и шкала оценивания (выполнение практических заданий)

«отлично» - по решению задачи дан правильный ответ и развернутый вывод
«хорошо» - по решению задачи дан правильный ответ, но не сделан вывод
«удовлетворительно» - по решению задачи дан частичный ответ, не сделан вывод
«неудовлетворительно» - задача не решена полностью