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: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
15 мая 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ОСНОВЫ КОМПЬЮТЕРНЫХ НАУК
«Б1.О.05.03 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) подготовки: Разработка программного обеспечения для обработки и анализа пространственных данных

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года

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

Москва, 2026

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Пучин В. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922

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	05.11.2025, № 12-25

Содержание

1. Цель и задачи освоения дисциплины (модуля)

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

3. Место дисциплины в структуре ОП

4. Объем дисциплины и виды учебной работы

5. Содержание дисциплины
   5.1. Разделы, темы дисциплины и виды занятий
   5.2. Содержание разделов, тем дисциплины и формы текущего контроля

6. Оценочные материалы текущего контроля

7. Оценочные материалы промежуточной аттестации

8. Порядок проведения промежуточной аттестации

9. Материально-техническое и учебно-методическое обеспечение дисциплины
   9.1. Перечень основной и дополнительной учебной литературы
   9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
   9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
   9.4. Оборудование и технические средства обучения

10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся целостного представления о роли информационной безопасности и способности анализировать последствия типовых информационных угроз для объекта защиты.

Задачи изучения дисциплины:

- изучить базовые понятия, цели и задачи информационной безопас-ности;
- рассмотреть основные положения Доктрины информационной безопасности Российской Федерации;
- освоить базовые механизмы идентификации, аутентификации, ав-торизации и управления доступом;
- сформировать представление о криптографических, сетевых и про-граммно-технических средствах защиты информации;
- применить изученные подходы при анализе учебных ситуаций и настройке средств защиты в изолированной среде.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.4 Реализует базовые меры и принципы обеспечения информационной безопасности при работе с данными, информационными системами и сетевыми ресурсами

Знать:

ОПК-3.4/Зн1 Основные принципы информационной безопасности

Уметь:

ОПК-3.4/Ум1 Применять меры защиты данных

ОПК-3.4/Ум2 Настраивать базовую безопасность систем

Владеть:

ОПК-3.4/Нв1 Навыками реализации мер защиты информации в повседневной работе

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.05.03 «Основы информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 7.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период	доемкость сы)	доемкость ЗЕТ)	ые занятия сы)	кие занятия сы)	ьная работа сы)	ая аттестация сы)

обучения	Общая тру (ча	Общая тру (ЗЕ	Лекционни (ча	Практическ (ча	Самостоятел (ча	Промежуточн (ча
7 семестр	108	3	18	38	25	Экзамен (27)
Всего	108	3	18	38	25	27

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Роль информационной безопасности и базовые организационные положения	**16**	**4**	**8**	**4**	ОПК-3.4
Тема 1.1. Введение в специальность «специалист по информационной безопасности»	8	2	4	2	
Тема 1.2. Доктрина информационной безопасности Российской Федерации	8	2	4	2	
Раздел 2. Управление доступом и основы криптографической защиты	**35**	**8**	**16**	**11**	ОПК-3.4
Тема 2.1. Идентификация, аутентификация и авторизация	11	2	6	3	
Тема 2.2. Авторизация и контроль доступа	12	2	6	4	
Тема 2.3. Основы криптографии	12	4	4	4	
Раздел 3. Сетевые технологии и средства защиты информации	**30**	**6**	**14**	**10**	ОПК-3.4
Тема 3.1. Основы сетей: модель OSI и стек протоколов TCP/IP	12	2	6	4	
Тема 3.2. IP-адресация и основные сетевые устройства	10	2	4	4	
Тема 3.3. Средства защиты информации	8	2	4	2	
Итого	**81**	**18**	**38**	**25**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Роль информационной безопасности и базовые организационные положения

Тема 1.1. Введение в специальность «специалист по информационной безопасности»

Понятие информационной безопасности. Объекты защиты. Основные виды угроз и последствий. Профессиональные задачи и этические требования к специалисту по информационной безопасности.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 1.2. Доктрина информационной безопасности Российской Федерации

Национальные интересы в информационной сфере, основные угрозы, стратегические цели и направления обеспечения информационной безопасности.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Управление доступом и основы криптографической защиты

Тема 2.1. Идентификация, аутентификация и авторизация

Назначение идентификаторов. Факторы аутентификации. Многофакторная аутентификация. Жизненный цикл учетных записей и базовые риски компрометации.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 2.2. Авторизация и контроль доступа

Субъекты и объекты доступа. Принцип минимальных привилегий. Дискреционная, мандатная и ролевая модели управления доступом.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 2.3. Основы криптографии

Назначение шифрования, хеширования, электронной подписи и управления ключами. Симметричные и асимметричные криптографические преобразования.

Текущий контроль

Вид (форма) контроля
Тестирование

Практическая работа

Раздел 3. Сетевые технологии и средства защиты информации

Тема 3.1. Основы сетей: модель OSI и стек протоколов TCP/IP

Уровни сетевого взаимодействия, назначение основных протоколов и типовые угрозы, возникающие при передаче информации.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 3.2. IP-адресация и основные сетевые устройства

Адресация IPv4 и IPv6, подсети, широковещательные домены, назначение коммутаторов, маршрутизаторов и межсетевых экранов.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 3.3. Средства защиты информации

Организационные, программные, программно-аппаратные, технические и криптографические средства защиты. Многоуровневая защита объекта информатизации.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

6. 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, 7 семестр.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения

обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

7. Оценочные материалы текущего контроля

Раздел 1. Роль информационной безопасности и базовые организационные положения
Контролируемые ИДК: ОПК-3.4

Тема 1.1. Введение в специальность «специалист по информационной безопасности»

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Нужно оценить ущерб после ошибочного удаления файла. Пока неизвестно, какой файл удален и для чего он использовался.

А. Определить его назначение в работе
Б. Установить удаленный объект
В. Описать нарушенное действие и последствие

2. Установите порядок зависимых действий. Разрешена только учебная проверка по заранее согласованному плану; выполнять ее до согласования нельзя. Результат документируют по фактическому наблюдению.

А. Зафиксировать разрешенные границы проверки
Б. Записать наблюдение и пределы вывода
В. Выполнить согласованную проверку

3. Сервис был недоступен с 10:00 до 10:25; прием заявок полностью зависит от него. Сколько минут длился подтвержденный перерыв приема?

4. В записи о заказе сумма была 500, после ошибочного изменения стала 50. На сколько уменьшено значение?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Последствия трех событий в службе обращений

По учебному описанию службы рассмотрите отправку закрытой карточки постороннему, ошибочное изменение срока и остановку приема. Для каждого события укажите объект, нарушенное свойство, затронутое рабочее действие и подтвержденное либо предполагаемое последствие; предположение обозначьте явно.

2. Границы разрешенной учебной проверки

Подготовьте план безопасной проверки доступа к копии отчета. Укажите разрешенный объект, фиктивные данные, действие проверки и условие остановки. Разберите, какие последствия возможны при ошибочном переносе того же действия на рабочую систему без согласования.

Тема 1.2. Доктрина информационной безопасности Российской Федерации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. При разборе Доктрины рассматривают защиту личной переписки. Пункт выбирают после определения затронутого интереса, а вывод основывают на выбранном пункте.

А. Найти соответствующее положение Доктрины
Б. Определить затронутый интерес
В. Объяснить связь случая с найденным положением

2. Установите порядок зависимых действий. Группа готовит краткую справку по Доктрине. Ссылки допустимы лишь после сверки текста документа, итог пишут по сверенным положениям.

А. Выбрать и сверить нужные пункты
Б. Составить справку с точными ссылками
В. Проверить название и реквизиты документа

3. Доктрина описывает официальные взгляды на национальную безопасность в определенной сфере. Назовите эту сферу.

4. Каким должностным лицом утверждена Доктрина информационной безопасности Российской Федерации 2016 года?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Положения Доктрины в учебных ситуациях

Найдите в тексте Доктрины положения о защите частной жизни и устойчивости инфраструктуры. Свяжите их с двумя вымышленными ситуациями: раскрытием личного сообщения и остановкой сервиса обращений. Для каждой связи укажите точный пункт и объясните затронутый интерес своими словами.

2. Силы, средства и результат совместной работы

Для учебной организации опишите, кто уполномочен отвечать за прием сообщений о сбое, какие организационные и технические средства ему нужны и какой результат должен быть достигнут. Разберите последствие ситуации, когда средство имеется, но ответственное лицо и порядок работы не определены. Отдельно свяжите подготовку специалиста с целью и одним направлением в области науки и образования из пп.26–27 Доктрины.

Раздел 2. Управление доступом и основы криптографической защиты

Контролируемые ИДК: ОПК-3.4

Тема 2.1. Идентификация, аутентификация и авторизация

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. В учебной системе сеанс допускается только после проверки заявленной учетной записи; доступ к документу проверяют уже для подтвержденного пользователя.

А. Проверить подтверждение принадлежности записи
Б. Проверить разрешение на документ
В. Предъявить идентификатор учетной записи

2. Установите порядок зависимых действий. Для замены утраченного фактора установлен порядок: новый фактор можно привязать только после проверки владельца, а проверочный вход выполняют после завершения замены.

А. Проверить вход с новым фактором
Б. Проверить владельца по разрешенной процедуре
В. Заменить привязку утраченного фактора

3. Учебное правило приостанавливает новые попытки после третьего подряд неверного ввода. Уже было два неверных ввода. Сколько еще неверных вводов достигнет порога?

4. Из десяти активных учетных записей подтверждена текущая работа владельцев восьми. У двух остальных работа завершена. Сколько записей требуют проверки и прекращения ненужного доступа?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Три разных решения при входе

Опишите простой вход в учебный сервис и обращение к закрытому отчету. Отметьте отдельно предъявление имени, проверку личности и решение о праве на отчет. Разберите случай, когда личность подтверждена, но отчет принадлежит другой рабочей группе.

2. Независимость факторов и восстановление доступа

Сравните пароль с PIN и пароль с зарегистрированным аппаратным фактором. Укажите категории факторов и разберите потерю устройства. Составьте простую схему восстановления, в которой замена привязки не выполняется до проверки владельца.

Тема 2.2. Авторизация и контроль доступа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Матрицу прав нужно разработать до настройки; проверяют уже примененный набор разрешений.

А. Определить рабочие действия роли
Б. Проверить разрешенное и запрещенное действия
В. Задать по ним минимальные права

2. Установите порядок зависимых действий. Роль еще не создана. Назначение пользователя допускается только после настройки прав этой роли.

А. Создать роль для рабочей функции
Б. Назначить пользователю подготовленную роль
В. Закрепить за ролью нужные разрешения

3. Роль должна читать и создавать обращения. Ей выданы чтение, создание, удаление и изменение настроек. Сколько лишних действий указано?

4. Роль editor разрешает чтение и изменение, роль viewer — только чтение. Пользователь состоит в обеих ролях; разрешения складываются. Сколько разных действий ему доступно?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Матрица прав двух рабочих ролей

Для читателя и редактора двух учебных отчетов задайте права чтения и изменения по приведенным обязанностям. Найдите лишнее разрешение в выданной матрице и предложите исправление. Составьте по одному положительному и отрицательному примеру проверки.

2. Сравнение трех моделей управления доступом

Разберите три самостоятельных примера: владелец выдает доступ; правило сравнивает метку и допуск; сотрудник получает полномочия через роль. Для каждого укажите, кто задает решение и что произойдет при попытке обычного пользователя самостоятельно передать право. Примените заданное простое правило допуска к трем документам.

Тема 2.3. Основы криптографии

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Эталонный хеш разрешено фиксировать только с проверенной исходной копии. Передача допускается после защищенной фиксации эталона.

А. Вычислить хеш проверенной исходной копии
Б. Передать файл и сравнить хеш полученной копии с эталоном
В. Зафиксировать эталон в доверенном месте

2. Установите порядок зависимых действий. Данные пока не зашифрованы. Перед созданием шифрованной копии должен быть определен доступный способ защищенного хранения и восстановления ключа; затем проверяют чтение копии.

А. Создать учебную шифрованную копию
Б. Проверить ее чтение уполномоченным получателем
В. Определить защищенное хранение и восстановление ключа

3. У двух копий одного файла разные значения SHA-256, вычисленные над полным содержимым. Какое отношение их байтового содержимого установлено?

4. Закрытый архив зашифрован, а единственная копия ключа потеряна. Какую возможность для уполномоченного пользователя поставили под угрозу?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Хеш и доверенный эталон

Для трех коротких фиктивных сообщений сравните выданные или вычисленные SHA-256: два одинаковых сообщения и одно измененное. Объясните, что устанавливает сравнение с доверенным эталоном, и отдельно разберите получение файла и хеша из одного недоверенного места.

2. Средства для закрытого и подписанного документа

Для двух целей — скрыть содержание от постороннего и проверить происхождение подписанных данных — выберите соответствующие механизмы. На схеме отметьте открытые и секретные компоненты ключей и разберите последствия потери единственного ключа расшифрования и раскрытия ключа подписи.

Раздел 3. Сетевые технологии и средства защиты информации

Контролируемые ИДК: ОПК-3.4

Тема 3.1. Основы сетей: модель OSI и стек протоколов TCP/IP

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Расположите три нижних уровня OSI от физической среды вверх.

А. Сетевой

Б. Физический
В. Канальный

2. Установите порядок зависимых действий. Прикладные закрытые данные по условию нельзя посылать до установления проверенного защищенного канала; результат получают после передачи.

А. Получить и обработать ответ
Б. Установить защищенный канал с проверкой стороны
В. Передать закрытые прикладные данные по этому каналу

3. Два сетевых сервиса работают на одном IP-адресе. Какое числовое поле TCP или UDP помогает указать сервис назначения?

4. Файл передан по защищенному каналу, но после получения его удалил пользователь конечного компьютера. На каком участке произошло событие, которое не предотвращает защита канала?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Сопоставление уровней сетевого обмена

На схеме отправки заявки отметьте приложение, транспорт, IP и локальную передачу. Для отключенного кабеля и неверного межсетевого пути укажите область первичной проверки. Сопоставьте нижние уровни OSI с их обязанностями, не утверждая полного совпадения двух моделей.

2. Транспорт и защита содержания

Сравните два учебных требования: упорядоченный поток и отдельные датаграммы с допустимой потерей. Выберите подходящий транспорт для каждого условия. Дополнительно разберите, почему надежная доставка сама не скрывает содержание, и какой результат ожидается от защищенного канала.

Тема 3.2. IP-адресация и основные сетевые устройства

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Префикс подсети еще неизвестен. Принадлежность адреса проверяют только после получения адреса сети и префикса.

А. Проверить принадлежность адреса этой сети
Б. Получить адрес сети и длину префикса
В. Зафиксировать результат проверки

2. Установите порядок зависимых действий. В учебной модели таблица MAC-адресов уже известна, адрес назначения найден единственным образом; разрешенный выходной порт отличается от входного. Расположите зависимые операции передачи кадра.

А. Найти соответствующий выходной порт в таблице
Б. Передать кадр на найденный порт
В. Прочитать MAC-адрес назначения кадра

3. Каков адрес сети для узла 192.0.2.37 с префиксом /24?

4. В разрешенный диапазон 192.0.2.0/24 проверяются адреса 192.0.2.9, 192.0.2.70 и 198.51.100.9. Сколько адресов входят в него?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Адреса и границы учебных подсетей

Определите принадлежность нескольких адресов к 192.0.2.0/24 и 198.51.100.0/24, найдите сетевой адрес узла с префиксом /24. Сопоставьте сокращенную и полную записи одного IPv6-адреса. Разберите последствие ошибочного включения адреса в разрешенный диапазон.

2. Коммутация и маршрут

Для небольшой учебной схемы используйте готовую таблицу MAC-адресов и портов, чтобы выбрать порт известного адресата. Затем рассмотрите отправку в другую подсеть и укажите

функцию шлюза. Объясните, почему таблица локального коммутатора не заменяет межсетевой маршрут.

Тема 3.3. Средства защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Установите порядок зависимых действий. Нужно подобрать меры для конкретного риска, а не по названию продукта. Проверка должна соответствовать выбранной мере.

А. Выбрать меру, уменьшающую этот риск
Б. Проверить наблюдаемый результат ее действия
В. Описать угрозу и ее последствие

2. Установите порядок зависимых действий. Учебное исправление проверяют после применения; заключение составляют на основании этой проверки.

А. Выполнить контрольное безопасное действие
Б. Применить согласованное исправление защиты
В. Записать результат и оставшееся ограничение

3. План защиты содержит четыре меры. Для трех есть протокол проверки, для одной только запись «установлено». Сколько мер еще требуют подтверждения результата проверки?

4. На учебной схеме зашифрованная резервная копия и ее единственный ключ лежат в одной доступной постороннему папке. Какой секрет прежде всего нужно хранить отдельно с ограничением доступа?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Дополняющие меры защиты

Для хранения закрытых учебных документов подберите организационную, физическую и программную либо криптографическую меры. Для каждой укажите угрозу, ожидаемый результат, простую проверку и ограничение. Покажите один случай, в котором меры дополняют друг друга.

2. Проверка результата и остаточные ограничения

По учебному отчету «средство установлено» составьте полноценное заключение для одной угрозы: ожидаемое поведение, контрольное действие, фактическое наблюдение и ограничение вывода. Сравните два протокола, в одном из которых запрещенное действие прошло успешно.

8. Оценочные материалы промежуточной аттестации

7 семестр, Экзамен

Контролируемые ИДК: ОПК-3.4

Вопросы/Задания:

1. Что включает понятие информационной безопасности кроме конфиденциальности?

2. Чем содержание закрытого документа отличается от его носителя?

3. Чем слабое место отличается от последствия угрозы?

4. Почему специалист заранее согласует границы учебной проверки?

5. Почему после сбоя нужно назвать затронутую рабочую операцию?

6. Какое назначение Доктрины указано в ее начале?

7. Чьи потребности названы в определении национальных интересов информационной сферы?

8. Как защита личной переписки связана с Доктриной?

9. Чем силы обеспечения безопасности отличаются от средств?

10. Как подготовка специалиста связана с целью и направлениями Доктрины в науке и образовании?

11. Чем имя учетной записи отличается от доказательства ее принадлежности?

12. Почему пароль и PIN не образуют две независимые категории факторов?

13. Что опасно в замене второго фактора только по сообщенному имени?

14. Почему закрыть вкладку не всегда достаточно для выхода?

15. Какое последствие уменьшают ограничением частоты неудачных входов?

16. Кто является субъектом и что объектом при чтении сотрудником отчета?

17. Как объяснить выдачу только чтения вместо административной роли?

18. Как роль связывает пользователя с разрешениями?

19. Что показывает успешное запрещенное действие через прямой запрос?

20. Зачем при проверке матрицы нужны отрицательные примеры?

21. Чем ключи симметричной схемы отличаются от пары асимметричной?

22. Какие функции различают физический, канальный и сетевой уровни?

23. Чем надежность TCP отличается от простой передачи UDP-датаграмм?

24. Зачем сетевое взаимодействие описывают по уровням?

25. Сколько бит имеет адрес IPv4 и сколько IPv6?

26. Зачем вместе с IPv4-адресом знать длину префикса подсети?

27. Чем основная функция коммутатора второго уровня отличается от маршрутизатора?

28. Чем физическая защита носителя отличается от шифрования?

29. Почему установка средства не доказывает его полезную работу?

30. С чего начать выбор меры для неизвестной угрозы?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Титова Л. Н. Информационная безопасность и защита информации: учебно-методическое пособие / Л. Н. Титова. - Уфа: БГПУ имени М. Акмуллы, 2013. - 108 с. - Текст: электронный // Издательство Лань: [сайт]. - URL: http://e.lanbook.com/books/element.php?pl1_id=56704 - Режим доступа: по подписке

2. Аникин Д. В. Информационная безопасность и защита информации / Д. В. Аникин. - Санкт-Петербург: ИЭО СПбУТУиЭ, 2011. - 269 с. - 978-5-94047-394-7. - Текст: электронный // Издательство Лань: [сайт]. - URL: http://e.lanbook.com/books/element.php?pl1_id=63950 - Режим доступа: по подписке

3. Нестеров С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - 3-е изд., стер. - Санкт-Петербург: Лань, 2024. - 324 с. - 978-5-507-49077-6. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/370967 - Режим доступа: по подписке

Дополнительная литература

1. Башлы П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Информационная безопасность и защита информации - Москва: Евразийский открытый институт, 2012. - 311 с. - 978-5-374-00301-7. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/10677.html - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://e.lanbook.com/ - Электронная библиотечная система "Лань"
2. https://rusneb.ru/ - Национальная электронная библиотека (НЭБ)
3. https://urait.ru - Образовательная платформа «Юрайт»
4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю
5. https://owasp.org/www-project-web-security-testing-guide/ - OWASP Web Security Testing Guide
6. https://attack.mitre.org/ - MITRE ATT&CK
7. https://skillsforall.com/ - Cisco Skills for All

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс
Маркерная доска - 0 шт.
Моноблок - 96 шт.
Проектор - 6 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.