МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Программно-аппаратные средства защиты информации»

Специальность	Информационная безопасность автоматизированных систем
Направленность (профиль)	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	8

Предисловие

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Программно-аппаратные средства защиты информации». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины Программно-аппаратные средства защиты информации».

3. Разработчики: Орёл Д.В., - доцент кафедры организации и технологии защиты информации

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Бабенко М. Г.– зав. кафедрой вычислительной математики и кибернетики

Члены комиссии:
Пелешенко В. С. – доцент кафедры вычислительной математики и кибернетики
Пелешенко Т. А. – доцент кафедры вычислительной математики и кибернетики

Представитель организации-работодателя: Корниенко С.А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах.
Экспертное заключение: фонд оценочных средств соответствует образовательной программе по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	**Уровни сформированности компетенци(ий)**			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	**Минимальный уровень (удовлетворительно) 3 балла**	**Средний уровень (хорошо) 4 балла**	**Высокий уровень (отлично) 5 баллов**
Компетенция: **ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1$_{ОПК-2}$** Осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с	Не осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с операционной системой; выбирает методы мониторинга компонентов операционной системы Windows, а	На слабом уровне осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с операционной системой; выбирает методы мониторинга компонентов	В основном осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с операционной системой; выбирает методы мониторинга компонентов операционной системы Windows, а	Полностью осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с операционной системой; выбирает методы мониторинга компонентов операционной системы Windows, а также режимы

операционной системой; выбирает методы мониторинга компонентов операционной системы Windows, а также режимы отказоустойчивой конфигурации.	также режимы отказоустойчивой конфигурации.	операционной системы Windows, а также режимы отказоустойчивой конфигурации.	также режимы отказоустойчивой конфигурации.	отказоустойчивой конфигурации.
Результаты обучения по дисциплине: *Индикатор:* **ИД-2$_{ОПК-2}$** Устанавливает и удаляет операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программны	Не может устанавливать и удалять операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программный маршрутизатор на базе ОС Windows; диагностирует причины сбоев работоспособности	Не может устанавливать, но при этом может удалять операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программный маршрутизатор на базе ОС Windows; диагностируе	С небольшими сложностями устанавливает и удаляет операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программный маршрутизатор на базе ОС Windows; диагностирует причины сбоев работоспособн	Полностью контролирует установление и удаление операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программный маршрутизатор на базе ОС Windows; диагностирует причины сбоев работоспособно

й маршрутизатор на базе ОС Windows; диагностирует причины сбоев работоспособности операционной системы Windows с помощью системного программного обеспечения.	операционной системы Windows с помощью системного программного обеспечения.	т причины сбоев работоспособности операционной системы Windows с помощью системного программного обеспечения.	ости операционной системы Windows с помощью системного программного обеспечения.	сти операционной системы Windows с помощью системного программного обеспечения.
Результаты обучения по дисциплине: *Индикатор:* **ИД-З$_{ОПК-2}$** Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	Не способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	С грубыми ошибками способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	С ошибками способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	На высоком уровне способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.
Компетенция: **ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем**				

Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-15** Выделяет этапы разработки политики информационной безопасности для организации; осуществляет поиск особенностей подсистем защиты ОС Windows и Linux; осуществляет систематизацию стандартных средств организации виртуальных частных сетей; определяет различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений; выбирает стандартные схемы использования межсетевых экранов;	Не предоставляет отчет, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей, показывает различия в Особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты, распространенных СУБД	Предоставляет неполный отчет с неполным пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных СУБД.	Предоставляет отчет с пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты, распространенных СУБД.	Предоставляет детальный отчет с полным пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных СУБД.

выделяет особенности подсистем защиты, распространенных СУБД.				
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-15** Оценивает эффективность и надежность защиты ОС, ВС и СУБД; планирует политику безопасности организации; выявляет слабости защиты ОС, ВС и СУБД использовать их для вскрытия защиты; организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.	Не предоставляет отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ОС, ВС и СУБД; планировать политику безопасности организации, а также выявлять слабости защиты ОС, ВС и СУБД и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.	Предоставляет неполный отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ОС, ВС и СУБД; планировать политику безопасности организации, а также выявлять слабости защиты ОС, ВС и СУБД и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.	Предоставляет отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ОС, ВС и СУБД; планировать политику безопасности организации, а также выявлять слабости защиты ОС, ВС и СУБД и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.	Предоставляет детальный отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ОС, ВС и СУБД; планировать политику безопасности организации, а также выявлять слабости защиты ОС, ВС и СУБД и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам

Результаты обучения по дисциплине: *Индикатор:* **ИД-3опк-15** Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.	Не предоставляет отчет, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Предоставляет неполный отчет с неполным пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Предоставляет отчет с м пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Предоставляет детальный отчет с полным пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
Компетенция: **ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем**				
Результаты обучения по дисциплине: *Индикатор:* **ИД-1опк-7.1** Способен оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информацио	Не предоставляет с оценкой информационных рисков в автоматизированных системах, определена информационная инфраструктура, нуждающаяся в защите.	Предоставляет неполный отчёт с оценкой информационных рисков в автоматизированных системах, определена информационная инфраструктура, нуждающаяся в защите.	Предоставляет отчёт по с оценкой информационных рисков в автоматизированных системах, определена информационная инфраструктура, нуждающаяся в защите.	Предоставлен детальный отчёт с оценкой информационных рисков в автоматизированных системах, определена информационная инфраструктура, нуждающаяся в защите.

нные ресурсы, подлежащие защите.				
Результаты обучения по дисциплине: *Индикатор:* **ИД-2опк-7.1** Формулирует угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в информационных системах.	Не предоставляет в котором представлены и сформулированы угрозы информационной безопасности, критерии оценки защищенности и представлены методы ЗИ в ИС.	Предоставляет неполный отчёт в котором представлены и сформулированы угрозы информационной безопасности, критерии оценки защищенности и представлены методы ЗИ в ИС.	Предоставляет отчёт в котором представлены и сформулированы угрозы информационной безопасности, критерии оценки защищенности и представлены методы ЗИ в ИС.	Предоставлен детальный отчёт, в котором представлены и сформулированы угрозы информационной безопасности, критерии оценки защищенности и представлены методы ЗИ в ИС.
Результаты обучения по дисциплине: *Индикатор:* **ИД-3опк-7.1** Осуществляет навыки разработки и исследования аналитических и компьютерных моделей информационных систем и подсистем безопасност	Не предоставляет с демонстрацией способности разрабатывать компьютерные модели и подсистемы безопасности ИС.	Предоставляет неполный отчёт с демонстрацией способности разрабатывать компьютерные модели и подсистемы безопасности ИС.	Предоставляет отчёт с демонстрацией способности разрабатывать компьютерные модели и подсистемы безопасности ИС.	Предоставляет детальный отчет с демонстрацией способности разрабатывать компьютерные модели и подсистемы безопасности ИС.

и информационных систем.				

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Семестр 8	
1.	b	Возможность за приемлемое время получить требуемую информационную услугу называется: a) Конфиденциальность b) Доступность c) Целостность d) Непрерывность	ОПК-2, ОПК -15, ОПК -7.1
2.	d	К аспектам информационной безопасности не относится: a) Доступность b) Целостность c) Конфиденциальность d) Защищенность	ОПК-2, ОПК -15, ОПК -7.1
3.	c	По каким критериям нельзя классифицировать угрозы: a) по расположению источника угроз b) по аспекту информационной безопасности, против которого угрозы направлены в первую очередь c) по способу предотвращения d) по компонентам информационных систем, на которые угрозы нацелены	ОПК-2, ОПК -15, ОПК -7.1
4.	a	Главное достоинство парольной аутентификации – … a) Простота b) Надежность c) Секретность d) запоминаемость	ОПК-2, ОПК -15, ОПК -7.1
5.	b	Сколько уровней включает в себя сетевая модель OSI? a) 5 b) 7 c) 6 d) 8	ОПК-2, ОПК -15, ОПК -7.1
6.	c	Межсетевой экран (Брандмауэр, firewall) – это…	ОПК-2, ОПК -15,

		a) Комплекс аппаратных средств b) Комплекс программных средств c) Комплекс аппаратных или программных средств d) Комплекс аппаратных и программных средств	ОПК -7.1
7.	a	На каком уровне сетевой модели OSI не работает межсетевой экран: a) Физический b) Сеансовый c) Сетевой d) Транспортный	ОПК-2, ОПК -15, ОПК -7.1
8.	b	Межсетевого экрана какого класса не существует: a) экранирующий маршрутизатор b) экранирующий коммутатор c) экранирующий транспорт d) экранирующий шлюз	ОПК-2, ОПК -15, ОПК -7.1
9.	d	Что из перечисленного не входит в состав программного комплекса антивирусной защиты: a) Подсистема сканирования b) Подсистема управления c) Подсистема обнаружения вирусной активности d) Подсистема устранения вирусной активности	ОПК-2, ОПК -15, ОПК -7.1
10.	c	На каком этапе заканчивается жизненный цикл автоматизированной системы? a) Бета-тестирование системы b) Внедрение финальной версии системы в эксплуатацию c) Прекращение сопровождения и технической поддержки системы d) Альфа-тестирование системы	ОПК-2, ОПК -15, ОПК -7.1
11.	d	Какие задачи выполняет теория защиты информации: a) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты b) аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации c) формировать научно обоснованные перспективные направления развития теории и практики защиты информации d) выполняет все вышеперечисленные	ОПК-2, ОПК -15, ОПК -7.1

12.	c	Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет: a) SSL b) SET c) HTTP d) IPSec	ОПК-2, ОПК -15, ОПК -7.1
13.	c	Какого метода разграничения доступа не существует: a) разграничение доступа по спискам b) разграничение доступа по уровням секретности и категориям c) локальное разграничение доступа d) парольное разграничение доступа	ОПК-2, ОПК -15, ОПК -7.1
14.	d	К основным функциям подсистемы защиты операционной системы относятся: a) идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа b) криптографические функции c) сетевые функции d) все вышеперечисленные	ОПК-2, ОПК -15, ОПК -7.1
15.	b	Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в ... a) системный блок b) сетевые операционные системы c) Microsoft Office 2013 d) операционную систему MS DOS	ОПК-2, ОПК -15, ОПК -7.1
16.	a, b	Что относится к аппаратным средствам защиты информации? a) электронные устройства b) электронно-механические устройства c) механические средства	ОПК-2, ОПК -15, ОПК -7.1
17.	b	Под этим применительно к обеспечению информационной безопасности компьютерной сети, понимают однозначное распознавание уникального имени субъекта компьютерной сети. a) Аутентификация b) Идентификация c) Протоколирование d) аудит	ОПК-2, ОПК -15, ОПК -7.1

18.	b	Характеризуется тем, что при шифровании используются два ключа: первый ключ делается общедоступным (публичным) и используется для шифровки, а второй является закрытым (секретным) и используется для расшифровки a) симметричное шифрование b) ассиметричное шифрование c) цифровая подпись	ОПК-2, ОПК -15, ОПК -7.1
19.	a	Какие задачи решают сетевые сканеры безопасности? a) идентификация и анализ уязвимостей b) инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети c) формирование отчетов, содержащих описание уязвимостей и варианты их устранения d) поиск и идентификация угроз в сети интернет	ОПК-2, ОПК -15, ОПК -7.1
20.	a	Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. a) Зондирование b) Сканирование c) Поиск d) протоколирование	ОПК-2, ОПК -15, ОПК -7.1
21.	a	Что является одним из главных требований к современным сетевым сканерам уязвимостей, помимо собственно безопасности? a) поддержка различных операционных систем b) способность обнаруживать все новые вирусы c) мультиязычность	ОПК-2, ОПК -15, ОПК -7.1
22.	a, b, c, d	К основным программным средствам защиты информации относятся: a) программы идентификации и аутентификации пользователей КС b) программы разграничения доступа пользователей к ресурсам КС c) программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования. d) программы шифрования информации e) программы кодирования информации	ОПК-2, ОПК -15, ОПК -7.1

23.	a	Как называют средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. a) Экран b) Шлюз c) Файервол d) Мост	ОПК-2, ОПК -15, ОПК -7.1
24.	a	Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. a) сканеры безопасности b) брандмауэры c) серверы	ОПК-2, ОПК -15, ОПК -7.1
25.	заключительном	Существующие механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа работают на … этапе осуществления атаки подготовительном основном	ОПК-2, ОПК -15, ОПК -7.1
26.	специализированных аппаратных средств со встроенными Шифропроцессорами	Наибольшая универсализация средств защиты реализована в VPN на основе …	ОПК-2, ОПК -15, ОПК -7.1
27.	Шлюз безопасности VPN	Сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним – это …	ОПК-2, ОПК -15, ОПК -7.1
28.	a, b, d	Какие меры по защите информации реализованы в ПАК «Аккорд»? a) Контроль целостности программ и данных, защита их от несанкционированной модификации b) Защита от несанкционированного доступа к ПЭВМ	ОПК-2, ОПК -15, ОПК -7.1

		c) Сканирование программного обеспечения на фактор угроз d) Управление терминальными сессиями	
29.	Резидентный компонент безопасности	**… – это встроенный в вычислительную систему объект, способный контролировать целостность среды путем сравнения ее параметров с эталонными.**	ОПК-2, ОПК -15, ОПК -7.1
30.	a, d	Какие меры по защите информации реализованы в ПАК «Соболь»? a) Обеспечение доверенной загрузки b) Защита от несанкционированного доступа к ПЭВМ c) Сканирование программного обеспечения на фактор угроз d) Идентификация и аутентификация пользователей по электронным идентификаторам	ОПК-2, ОПК -15, ОПК -7.1

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

3. Критерии оценивания компетенций

Оценка «**отлично**» выставляется студенту, если он: предоставляет отчёт с детальным анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства windows; методов инсталляции системного программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы windows, а также режимов отказоустойчивой конфигурации; предоставляет детальный отчёт с результатами установки и удаления операционной системы семейства windows, развертывания службы каталогов windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы windows. а также результатами использования программного маршрутизатора на базе ос windows; диагностики причин сбоев работоспособности операционной системы windows с помощью системного программного обеспечения; предоставляет детальный отчёт с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; предоставляет детальный отчет с полным пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ос windows и linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных субд; предоставляет детальный отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ос, вс и субд; планировать политику безопасности организации, а так же выявлять слабости защиты ос, вс и субд и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам; предоставляет детальный отчет с полным пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

Оценка «**хорошо**» выставляется студенту в случае, когда он предоставляет отчёт с анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства windows; методов инсталляции системного программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы windows, а также режимов отказоустойчивой конфигурации; предоставляет отчёт с результатами установки и удаления операционной системы семейства windows, развертывания службы каталогов windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы windows. а также результатами использования программного маршрутизатора на базе ос windows; диагностики

причин сбоев работоспособности операционной системы windows с помощью системного программного обеспечения; предоставляет с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; предоставляет отчет с пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ос windows и linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных субд; предоставляет отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ос, вс и субд; планировать политику безопасности организации, а так же выявлять слабости защиты ос, вс и субд и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам; предоставляет отчет с пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

Оценка «**удовлетворительно**» выставляется студенту, если он предоставляет отчёт с неполным анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства windows; методов инсталляции системного программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы windows, а также режимов отказоустойчивой конфигурации; предоставляет неполный отчёт с результатами установки и удаления операционной системы семейства windows, развертывания службы каталогов windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы windows. а также результатами использования программного маршрутизатора на базе ос windows; диагностики причин сбоев работоспособности операционной системы windows с помощью системного программного обеспечения; предоставляет неполный отчёт с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; предоставляет неполный отчет с неполным пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ос windows и linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных субд; предоставляет неполный отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ос, вс и субд; планировать политику безопасности организации, а так же выявлять слабости защиты ос, вс и субд и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам; предоставляет неполный отчет с неполным пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.

Оценка «**неудовлетворительно**» выставляется, если студент: не предоставляет отчёт с анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства windows; методов инсталляции системного

программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы windows, а также режимов отказоустойчивой конфигурации; не предоставляет отчёт с результатами установки и удаления операционной системы семейства windows, развертывания службы каталогов windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы windows. а также результатами использования программного маршрутизатора на базе ос windows; диагностики причин сбоев работоспособности операционной системы windows с помощью системного программного обеспечения; не предоставляет отчёт с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности; не предоставляет отчет, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ос windows и linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных субд; не предоставляет отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ос, вс и субд; планировать политику безопасности организации, а так же выявлять слабости защиты ос, вс и субд и пользовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам; не предоставляет отчет, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем.