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

Перспективные направления защиты информации

| | |
|---|---|
| Специальность | 10.05.03 Информационная безопасность автоматизированных систем |
| Направленность (профиль) | Анализ безопасности информационных систем |
| Год начала обучения | 2026 |
| Форма обучения | очная |
| Реализуется в семестрах | А |

**Предисловие**

1. Назначение: проведение текущего контроля успеваемости и промежуточной аттестации по дисциплине «Перспективные направления защиты информации».

2. ФОС является приложением к программе дисциплины «Перспективные направления защиты информации».

3. Разработчики:

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 рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Перспективные направления защиты информации».
«___»_____2026 г.

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: ПК-9* Способен формировать требования к защите информации в автоматизированных системах | | | | |
| Результаты обучения по дисциплине:<br>*Индикатор:*<br>**ИД-1$_{ПК-9}$**<br>Обосновывает необходимость защиты информации в автоматизированной системе. | Не предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе. | Предоставляет неполный отчет с обоснованием необходимости защиты информации в автоматизированной системе. | Предоставляет отчет с обоснованием необходимости защиты информации в автоматизированной системе. | Предоставляет детальный отчет с обоснованием необходимости защиты информации в автоматизированной системе. |
| Результаты обучения по дисциплине:<br>*Индикатор:*<br>**ИД-2$_{ПК-9}$**<br>Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой. | Не предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой. | Предоставляет неполный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой. | Предоставляет отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой. | Предоставляет детальный отчёт по результатам определения угроз безопасности информации, обрабатываемой автоматизированной системой. |
| Результаты обучения по дисциплине:<br>*Индикатор:*<br>**ИД-3$_{ПК-9}$**<br>Разрабатывает архитектуру системы защиты информации автоматизированной системы. | Не предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы. | Предоставляет неполный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы. | Предоставляет отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы. | Предоставляет детальный отчёт по результатам разработки архитектуры системы защиты информации автоматизированной системы. |
| Результаты обучения по дисциплине:<br>*Индикатор:* | Не предоставляет отчёт по результатам моделирования | Предоставляет неполный отчёт по результатам | Предоставляет отчёт по результатам моделирования | Предоставляет детальный отчёт по результатам моделирования |

| | | | | |
|---|---|---|---|---|
| **ИД-4$_{ПК-9}$** Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации. | защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации. | моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации. | защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации. | защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации. |

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 А** | |
| 1 | 4 | Какое направление ИБ относится к перспективным?<br>1. Защита с помощью антивирусов<br>2. Применение межсетевых экранов<br>3. Контроль доступа по паролям<br>4. Использование искусственного интеллекта для выявления угроз | ПК-9 |
| 2 | 1 | Что такое квантовая криптография?<br>1. Метод шифрования, основанный на принципах квантовой механики<br>2. Новый вид симметричного шифрования<br>3. Алгоритм на основе искусственного интеллекта<br>4. Аппаратное средство защиты информации | ПК-9 |
| 3 | 3 | Какова основная цель Zero Trust-модели?<br>1. Упрощение доступа к сети<br>2. Централизованное управление ключами<br>3. Отсутствие доверия к любому пользователю и устройству по умолчанию<br>4. Быстрая идентификация по IP | ПК-9 |
| 4 | 2 | Что представляет собой блокчейн в контексте защиты информации?<br>1. Система хранения резервных копий<br>2. Распределённый журнал транзакций, обеспечивающий неизменность данных<br>3. База данных с ограниченным доступом<br>4. Виртуальный сервер для шифрования данных | ПК-9 |
| 5 | 1 | Какая технология позволяет выявлять аномалии в поведении пользователей в режиме реального времени?<br>1. Поведенческий анализ на базе машинного обучения<br>2. Сканирование портов<br>3. Фильтрация пакетов<br>4. Сегментация сети | ПК-9 |
| 6 | 4 | Что из перечисленного можно отнести к биометрической мультифакторной аутентификации? | ПК-9 |

| | | | |
|---|---|---|---|
| | | 1. PIN-код и токен<br>2. Пароль и CAPTCHA<br>3. Смарт-карта и логин<br>4. Отпечаток пальца и распознавание лица | |
| 7 | 3 | Какой подход используется в адаптивной кибербезопасности?<br>1. Проверка подписей файлов<br>2. Ограничение доступа по времени<br>3. Автоматическая корректировка защитных мер на основе текущей угрозы<br>4. Физическая защита сервера | ПК-9 |
| 8 | 2 | Что из нижеперечисленного является признаком внедрения технологии «конфиденциальных вычислений»?<br>1. Удалённое шифрование файлов<br>2. Защита данных в процессе их обработки<br>3. Аутентификация на основе сертификатов<br>4. Использование VPN | ПК-9 |
| 9 | 1 | Какой из методов подходит для безопасного обмена квантовыми ключами?<br>1. Протокол BB84<br>2. AES-256<br>3. SHA-3<br>4. RSA | ПК-9 |
| 10 | 3 | Что означает термин «гомоморфное шифрование»?<br>1. Метод визуального анализа данных<br>2. Шифрование только метаданных<br>3. Выполнение вычислений над зашифрованными данными без их расшифровки<br>4. Хеширование открытого текста | ПК-9 |
| 11 | 2 | Что такое SASE (Secure Access Service Edge)?<br>1. Устройство безопасности на периметре сети<br>2. Облачная архитектура, объединяющая функции сетевой и информационной безопасности<br>3. Протокол туннелирования<br>4. Система обнаружения атак на сервер | ПК-9 |
| 12 | 1 | Что позволяет реализовать технология AI-driven SOC (Security Operations Center)?<br>1. Автоматический анализ инцидентов безопасности на основе ИИ | ПК-9 |

| | | | |
|---|---|---|---|
| | | 2. Обновление антивирусов вручную<br>3. Управление хранилищем данных<br>4. Резервное копирование | |
| 13 | 4 | Что из нижеперечисленного представляет собой перспективный подход к защите IoT-устройств?<br>1. Физическая изоляция устройств<br>2. Ограничение MAC-адресов<br>3. Использование FTP для обновлений<br>4. Встраивание механизмов безопасности на уровне микропрограммного обеспечения | ПК-9 |
| 14 | 2 | Что означает термин «приватные блокчейны»?<br>1. Открытая децентрализованная платформа<br>2. Блокчейн-сеть с ограниченным доступом участников<br>3. Уязвимая система для хранения файлов<br>4. Публичный сервис обмена данными | ПК-9 |
| 15 | 3 | Что характеризует подход Security by Design?<br>1. Внедрение антивируса на финальной стадии разработки<br>2. Периодическое тестирование ПО<br>3. Проектирование системы с учётом безопасности на всех этапах разработки<br>4. Хранение логов в облаке | ПК-9 |
| 16 | 1 | Что такое цифровая идентичность (Digital Identity)?<br>1. Совокупность цифровых данных, позволяющих идентифицировать пользователя<br>2. Способ подделки логина<br>3. Уникальный IP-адрес<br>4. Аппаратный модуль безопасности | ПК-9 |
| 17 | 2 | Что представляет собой автоматизированный ответ на инциденты (SOAR)?<br>1. Вирусная активность в сети<br>2. Система автоматизации реагирования и координации действий при инцидентах ИБ<br>3. Модель межсетевого экрана<br>4. Методика анализа угроз | ПК-9 |
| 18 | 3 | Какой термин описывает потенциальную опасность применения ИИ в кибербезопасности?<br>1. Квантовая угроза<br>2. Блокчейн-конфликт<br>3. Атака с применением генеративного ИИ (AI-powered attack) | ПК-9 |

| | | | |
|---|---|---|---|
| | | 4. Флуд-инцидент | |
| 19 | 1 | Что входит в концепцию кибергигиены?<br>1. Регулярное обновление ПО, использование сложных паролей, внимательность к фишингу<br>2. Принудительная установка антивируса<br>3. Хранение информации на физических носителях<br>4. Удаление всех облачных сервисов | ПК-9 |
| 20 | 4 | Какой из нижеуказанных подходов обеспечивает защиту данных в облачной инфраструктуре?<br>1. Использование общедоступных хранилищ<br>2. Передача данных в открытом виде<br>3. Физическое копирование данных<br>4. Шифрование данных на клиентской стороне до передачи в облако | ПК-9 |

**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 «**зачтено**» выставляется студенту, если студент знает ключевых понятия, демонстрирует понимание основных терминов, принципов и теоретических основ дисциплины, материал излагается логично, с выделением причинно-следственных связей и примеров, используются рекомендованные учебные материалы, а также дополнительные достоверные источники, работы (индивидуальные, групповые, проектные) сданы в установленные сроки и соответствуют требованиям, студент корректно использует изученные методики, инструменты или технологии, в работах присутствуют обоснованные заключения, а в случае проектов – практическая значимость.

Оценка «**не зачтено**» выставляется студенту в следующих случаях: неудовлетворительное освоение программы: не продемонстрировано понимание базовых понятий и принципов дисциплины в работах содержатся грубые теоретические ошибки отсутствует логика в изложении материала ответы не соответствуют поставленным вопросам, невыполнение практических требований: работа не сдана в установленный срок без уважительной причины практические задания выполнены менее чем на 50% от требуемого объема нарушены методические требования к оформлению работ обнаружен плагиат (более 50% заимствованного текста без указания источников).