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

УТВЕРЖДАЮ
Декан факультета математики и
компьютерных наук
к. физ.-мат. н., доцент Гробова Т.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Аутентификация в киберфизических системах

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	3

Ставрополь 2026 г.

Введение

1. Назначение: данный фонд оценочных предназначен для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» по дисциплине «Аутентификация в киберфизических системах».

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины «Аутентификация в киберфизических системах» в соответствии с образовательной программой 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность» по дисциплине «Аутентификация в киберфизических системах».

3. Разработчик: к.т.н., доцент Рачков Валерий Евгеньевич, доцент кафедры организации и технологии защиты информации.

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены экспертной группы: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком-С»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.04.01 Информационная безопасность, направленность (профиль) «Информационная безопасность киберфизических систем» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Аутентификация в киберфизических системах».

5.Срок действия ФОС: на срок реализации образовательной программы.

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

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетвори тельно) 2 балла	Минимальный уровень (удовлетворител ьно) 3 балла	Минимальный уровень не достигнут (неудовлетвори тельно) 2 балла	Высокий уровень (отлично) 5 баллов
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах				
ПК-2 ИД-1 осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизически х системах	на низком уровне осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизически х системах	в основном осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизически х системах	может осуществлять анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизически х системах	на высоком профессионально м уровне осуществляет анализ особенностей проектирования и реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-2 проектирует и реализует политики безопасности вычислительных сетей в киберфизически х системах	на низком уровне проектирует и реализует политики безопасности вычислительных сетей в киберфизически х системах	в основном проектирует и реализует политики безопасности вычислительных сетей в киберфизически х системах	умеет проектировать и реализовать политики безопасности вычислительных сетей в киберфизически х системах	на высоком профессионально м уровне проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-4 формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизически х системах	на низком уровне формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизически х системах	в основном формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизически х системах	может формализовать результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизически х системах	на высоком профессионально м уровне формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем				
ПК-3 ИД-1 состав, порядок функционирован	на низком уровне: знает состав, порядок	в основном знает состав, порядок функционирован	знает состав, порядок функционирован	на высоком профессионально м уровне знает

ия и алгоритм построения системы управления информационной безопасностью киберфизических систем	функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	ия и алгоритм построения системы управления информационной безопасностью киберфизических систем	ия и алгоритм построения системы управления информационной безопасностью киберфизических систем	состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем
ПК-3 ИД-2 анализ уязвимости и построение модели угроз для киберфизических систем	на низком уровне: умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	в основном умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем	на высоком профессиональном уровне умеет анализировать уязвимости и проводить построение модели угроз для киберфизических систем
ПК-3 ИД-6 формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	на низком уровне формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	в основном формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	умеет формализовать методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне формализует методологию разработки предложений при совершенствовании системы управления информационной безопасностью киберфизических 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
		Форма обучения очная, семестр 3	
1.	b	Что, согласно современным методологиям, является основой для построения адаптивных алгоритмов аутентификации в КФС? a) Статический список разрешенных идентификаторов. b) **Формирование профиля субъекта доступа, учитывающего его поведенческие характеристики.** c) Обязательное использование только одноразовых паролей (OTP). d) Полный отказ от многофакторной аутентификации.	ПК-2
2.	b	Какое ключевое преимущество дает использование методологии профилей доступа в КФС? a) Упрощение процедуры входа в систему за счет сокращения количества паролей. **b) Возможность дифференцированной разработки адаптивных алгоритмов для проверки легитимности операций в режиме, близком к реальному времени.** c) Полное устранение необходимости в криптографической защите каналов связи. d) Снижение требований к вычислительным ресурсам конечных устройств.	ПК-2
3.	b	В чем заключается основной недостаток традиционных методов аутентификации применительно к современным КФС? a) Они требуют слишком много вычислительных ресурсов. **b) Они не позволяют противостоять ранее неизвестным атакам, угрозы от которых невозможно формализовать и описать определенными сигнатурами.** c) Они не поддерживают работу с биометрическими данными. d) Они несовместимы с беспроводными протоколами передачи данных.	ПК-2

4.	b	Какой подход лежит в основе методологии «Конструктивной кибербезопасности» (Secure by Design) при проектировании политики безопасности КФС? a) Безопасность настраивается как дополнительный модуль после завершения разработки системы. **b) Меры безопасности закладываются на уровне архитектуры и дизайна системы, являясь ее неотъемлемой частью.** c) Безопасность обеспечивается исключительно физическими средствами защиты. d) Политика безопасности разрабатывается только после первого инцидента.	ПК-2
5.	b	Какой принцип является одним из ключевых при проектировании политики безопасности для КФС в соответствии с методологией Security by Design? a) Принцип всеобщего доступа (Universal Access). **b) Принцип минимальных прав (Least Privilege).** c) Принцип единого окна (Single Window). d) Принцип максимального удобства пользователя (Maximum Convenience).	ПК-2
6.	b	Какая особенность накладывает наиболее существенные ограничения на выбор протоколов аутентификации для промышленных КФС? a) Высокая стоимость внедрения криптографических алгоритмов. **b) Жесткие ограничения на длину передаваемых данных и вычислительные возможности встраиваемых устройств.** c) Отсутствие необходимости в защите от несанкционированного доступа. d) Исключительно проводной тип соединения между компонентами.	ПК-2
7.	b	Что из перечисленного является характерной особенностью аутентификации в децентрализованных киберфизических средах? a) Наличие единого центрального сервера аутентификации. **b) Необходимость реализации междоменной аутентификации и аутентификации при передаче данных.** c) Отсутствие необходимости в защите от атак типа «человек посередине» (MitM). d) Использование только симметричных криптосистем.	ПК-2

8.	b	Какая тенденция в области аутентификации является наиболее актуальной для КФС в контексте новейших киберугроз? a) Возврат к текстовым паролям как к наиболее простому методу. **b) Активное внедрение беспарольных методов аутентификации.** c) Полный отказ от всех видов сетевой аутентификации. d) Использование единого статического ключа для всех устройств системы.	ПК-2
9.	b	Какой подход к аутентификации является основополагающим для концепции Zero Trust (нулевого доверия) в сетях 6G и КФС? a) Доверие ко всем устройствам, находящимся внутри периметра сети. **b) Непрерывная аутентификация, строгий контроль доступа и обнаружение аномалий в реальном времени.** c) Разовое подтверждение личности при подключении к сети. d) Использование только аппаратных токенов без проверки пользователя.	ПК-2
10.	a	Какой протокол, согласно ГОСТ Р 71252-2024, рекомендуется для использования в индустриальных системах с жесткими ограничениями на длину передаваемых данных? **a) Протокол CRISP.** b) Протокол TLS 1.3. c) Протокол OAuth 2.0. d) Протокол Kerberos.	ПК-2
11.	b	В чем заключается основное различие между технологиями PKI и FIDO с точки зрения аутентификации? a) PKI использует симметричную криптографию, а FIDO — асимметричную. **b) Обе используют асимметричную криптографию, но применяют разные схемы аутентификации.** c) FIDO не является криптографическим протоколом. d) PKI не поддерживает цифровые подписи.	ПК-2
12.	b	Какая задача решается с помощью протоколов группового согласования ключей (GKA) для шин киберфизических систем?	ПК-2

		a) Передача видеоданных высокого разрешения. **b) Динамическое согласование общего ключа между устройствами для обеспечения целостности и подлинности сообщений с помощью кодов аутентификации (MAC).** c) Синхронизация времени на всех устройствах сети. d) Дистанционное обновление прошивки на устройствах.	
13.	b	Какое требование является критически важным для протоколов аутентификации в мобильных КФС с ограниченными ресурсами (resource-constrained)? a) Поддержка высокого сетевого трафика. **b) Постквантовая устойчивость и низкое потребление ресурсов (lightweight и quantum-resistant).** c) Сложная инфраструктура открытых ключей (PKI). d) Обязательное наличие биометрического сканера на каждом устройстве	ПК-2
14.	a	Какой протокол аутентификации использует технологию распределенного реестра (DLT) для создания системы на основе одноразового ключа (AFOTAK)? **a) Рекомендация ITU-T X.1284.** b) Стандарт IEEE 802.1X. c) Протокол RADIUS. d) Протокол CHAP.	ПК-2
15.	b	Какое ключевое свойство обеспечивает использование цифровой подписи для цифровых двойников (Digital Twins) в КФС? a) Сжатие данных. **b) Масштабируемую аутентификацию, целостность и неотказуемость (non-repudiation).** c) Увеличение скорости передачи данных. d) Снижение энергопотребления.	ПК-2
16.	a	Какая технология была разработана в МФТИ для создания коллективной цифровой подписи, устойчивой к взлому с помощью квантовых компьютеров?	ПК-2

		a) Метод, позволяющий группе участников создавать единую подпись, где ни один из них не обладает полным секретным ключом. b) Метод подписи с открытым ключом на основе алгоритма RSA-4096. c) Схема слепой подписи (Blind Signature). d) Протокол подписи на основе кодов, исправляющих ошибки.	
17.	a	Каким свойством обладает детерминированная электронная подпись? **a) Она всегда одинакова для одного и того же сообщения, что упрощает управление документами.** b) Она генерируется случайным образом при каждой операции подписания. c) Она не требует использования закрытого ключа. d) Она может быть подделана любым пользователем системы.	ПК-2
18.	a	Какой стандарт определяет процессы генерации и проверки электронной подписи на основе эллиптических кривых в Российской Федерации? **a) ГОСТ 34.10-2018.** b) ISO/IEC 27001. c) ГОСТ 28147-89. d) RFC 5280 (PKIX).	ПК-2
19.	b	Что является обязательным требованием при реализации цифровых подписей с использованием USB-ключей PKCS#11 и HSM в корпоративных КФС? a) Отказ от аппаратной защиты ключей. **b) Обеспечение безопасности на аппаратном уровне (Hardware Security Module).** c) Использование только программных хранилищ ключей. d) Обязательное наличие интернет-соединения для проверки подписи.	ПК-2
20.	a	Какая процедура реализуется на первом этапе при использовании расширенного механизма аутентификации устройств на основе PKI? **a) Взаимная аутентификация с помощью цифровых сертификатов в начале сеанса связи.** b) Передача пароля в открытом виде.	ПК-2

		c) Отправка хеша от устройства без проверки сервера. d) Аутентификация только по MAC-адресу.	
21.	b	В чем заключается основная уязвимость традиционных методов аутентификации в КФС, которую решает использование физического уровня? a) Сложность интеграции с облачными сервисами. **b) Зависимость от выборки данных о нелегитимных пользователях, что приводит к неизбежным ошибкам обнаружения.** c) Высокая стоимость реализации. d) Отсутствие поддержки беспроводных интерфейсов.	ПК-2
22.	a	Какая схема подписи предлагается для защиты сообщений R-GOOSE и R-SV в стандарте IEC 61850? **a) Цифровая подпись на основе алгоритма FALCON (FDSS).** b) Подпись на основе алгоритма SHA-256. c) Схема подписи Эль-Гамаля. d) Цифровая подпись на основе алгоритма DSA.	ПК-2
23.	b	Какую функцию выполняют коды аутентификации сообщений (MAC) в протоколах группового согласования ключей для шин КФС? a) Шифрование полезной нагрузки. **b) Обеспечение целостности и подлинности сообщений между устройствами.** c) Сжатие передаваемых пакетов. d) Маршрутизация трафика между сегментами сети.	ПК-2
24.	b	Какую проблему решает использование постквантовой криптографии (PQC) для цифровых подписей в КФС? a) Увеличение скорости вычислений на 50%. **b) Обеспечение долгосрочной безопасности и устойчивости к атакам с использованием квантовых компьютеров (forward-secure и breach resiliency).** c) Снижение энергопотребления устройств.	ПК-2

		d) Упрощение процесса управления ключами.	
25.	b	Какое направление совершенствования СУИБ КФС является наиболее перспективным согласно современным методологиям? a) Увеличение длины паролей пользователей. **b) Внедрение адаптивных алгоритмов верификации, основанных на проактивном обнаружении атак и профилях поведения.** c) Полный отказ от аутентификации в пользу физической изоляции сетей. d) Централизация всех процессов аутентификации на одном сервере.	ПК-3
26.	a	Какой подход к формированию политик безопасности рекомендуется для повышения устойчивости КФС к гибридным и постквантовым угрозам? a) Построение многоуровневой (многоконтурной) системы информационной безопасности. b) Использование единого пароля для всех компонентов системы. c) Полный отказ от криптографических методов защиты. d) Периодическое отключение всех систем безопасности для обновления.	ПК-3
27.	b	Какое усовершенствование методологии оценки угроз является критически важным для КФС? a) Оценка угроз только на этапе ввода системы в эксплуатацию. **b) Внедрение оценки рисков аномального поведения пользователей в режиме, близком к реальному времени.** c) Игнорирование физических угроз для компонентов системы. d) Оценка только внешних сетевых атак.	ПК-3
28.	b	Какое свойство современных платформ управления киберфизическими объектами необходимо развивать для повышения адаптивности СУИБ? a) Жесткая централизация всех функций управления. **b) Эмерджентные системные свойства: киберустойчивость, самоорганизация и адаптивность.** c) Полная автономность без возможности удаленного управления. d) Снижение количества собираемых данных о состоянии системы.	ПК-3

29.	a	Какая интеграция методов защиты позволяет наиболее эффективно повысить уровень ИБ КФС согласно современным исследованиям? **a) Интеграция методов физической и логической защиты.** b) Разделение физической и кибернетической составляющих безопасности. c) Приоритет физической защиты над кибербезопасностью. d) Исключительно программные методы защиты без аппаратной составляющей.	ПК-3
30.	a	Какое усовершенствование системы аутентификации является наиболее актуальным для КФС с учетом роста числа «умных» устройств? **a) Переход от статических методов аутентификации к непрерывным и контекстно-зависимым.** b) Упрощение процедур аутентификации до однофакторных. c) Отказ от аутентификации для устройств интернета вещей (IoT). d) Использование единого неизменяемого идентификатора для всех устройств.	ПК-3
31.	b	Какая особенность КФС требует внедрения распределенных систем управления идентификацией и доступом (DID/SSI)? a) Малое количество узлов в сети. **b) Децентрализованный характер и необходимость междоменной аутентификации.** c) Отсутствие необходимости в защите персональных данных. d) Полная однородность всех устройств системы.	ПК-3
32.	a	Какую проблему решает внедрение проактивных алгоритмов обнаружения атак в СУИБ КФС? **a) Возможность противостоять ранее неизвестным атакам, которые невозможно описать определенными сигнатурами.** b) Увеличение времени реакции на известные угрозы. c) Снижение требований к квалификации персонала. d) Упрощение процедур аудита безопасности.	ПК-3

33.	b	Какое направление совершенствования аутентификации является ключевым для повышения безопасности мобильных КФС? a) Использование только длинных текстовых паролей. **b) Внедрение легковесных (lightweight) протоколов аутентификации для ресурсо-ограниченных устройств.** c) Отказ от шифрования для ускорения работы. d) Использование единого статического предустановленного ключа.	ПК-3
34.	b	Какая архитектурная особенность должна быть учтена при разработке предложений по совершенствованию СУИБ для КФС критической инфраструктуры? a) Полная изолированность от информационно-телекоммуникационных систем. **b) Объединение информационно-телекоммуникационных систем общего назначения и индустриальных сетей и устройств (контроллеров).** c) Отсутствие необходимости в защите от удаленных атак. d) Исключительно проводной тип соединения всех компонентов.	ПК-3
35.	a	Какое усовершенствование криптографических протоколов является приоритетным для повышения безопасности КФС в ближайшей перспективе? **a) Интеграция постквантовых криптоалгоритмов (PQC) в промышленные протоколы M2M-взаимодействия.** b) Отказ от асимметричной криптографии в пользу симметричной. c) Увеличение длины ключей RSA до 8192 бит. d) Переход на протоколы без установления сеансового ключа.	ПК-3
36.	a	Какое решение предлагается для повышения надежности групповой аутентификации на шинах КФС с распределенной топологией? **a) Внедрение аутентифицированных и полностью распределенных протоколов группового согласования ключей (GKA).** b) Использование предустановленных статических ключей на всех устройствах.	ПК-3

		c) Отказ от аутентификации на уровне шины данных. d) Использование единого пароля для всей группы устройств.	
37.	a	Какой инновационный подход к аутентификации предлагается для защиты от атак с использованием квантовых компьютеров в рамках протокола TLS 1.3? **a) Интеграция доказательств с нулевым разглашением (ZK-SNARK).** b) Увеличение размера заголовков TLS. c) Отказ от шифрования сеансового трафика. d) Использование только сертификатов X.509 без проверки.	ПК-3
38.	a	Какое усовершенствование протоколов аутентификации требуется для интеллектуальных транспортных систем? **a) Разработка протоколов, объединяющих криптографические гарантии с физическими доказательствами (местоположение и время).** b) Использование только одноразовых паролей, отправляемых по SMS. c) Отказ от взаимной аутентификации между транспортными средствами. d) Использование единого ключа для всех автомобилей в регионе.	ПК-3
39.	a	Какое направление развития криптографических протоколов для КФС поддерживается в рекомендации ITU-T X.1284? **a) Использование технологии распределенного реестра (DLT) для создания системы аутентификации на основе одноразового ключа (AFOTAK).** b) Возврат к использованию бумажных носителей ключевой информации. c) Отказ от стандартизации протоколов аутентификации. d) Использование только симметричных алгоритмов шифрования.	ПК-3
40.	a	Какое усовершенствование процедур цифровой подписи является критически важным для долгосрочной безопасности цифровых двойников (Digital Twins) в КФС? **a) Внедрение постквантовых и forward-secure (защищенных от компрометации в будущем) схем подписи.** b) Использование коротких ключей (менее 128 бит) для ускорения работы.	ПК-3

		c) Хранение закрытых ключей в открытом виде для упрощения доступа. d) Отказ от цифровой подписи в пользу контрольных сумм.	
41.	a	Какой метод совершенствования цифровой подписи устраняет риск кражи полного секретного ключа у одного из участников? **a) Использование коллективной (многосторонней) подписи, где ни один участник не обладает полным ключом.** b) Хранение ключа в файловой системе без шифрования. c) Использование одного и того же ключа для всех операций. d) Передача ключа по открытым каналам связи.	ПК-3
42.	a	Какое усовершенствование схемы цифровой подписи предлагается для распределенных систем с ограниченными ресурсами, таких как системы наблюдения за транспортными средствами? **a) Иерархическая многосторонняя цифровая подпись (HMPS) с модифицированной индивидуальной подписью на основе Эль-Гамаля.** b) Использование подписи на основе алгоритма MD5. c) Полный отказ от цифровой подписи из-за нехватки ресурсов. d) Централизованная подпись всех транзакций одним сервером.	ПК-3
43.	a	Какое свойство должны обеспечивать аппаратно-ассистированные эффективные подписи (HASES) для цифровых двойников в постквантовую эру? **a) Максимально легковесный характер (lightweight) при сохранении постквантовой устойчивости.** b) Использование исключительно программных методов генерации подписи. c) Отказ от защиты от квантовых атак. d) Обязательное наличие высокопроизводительного GPU.	ПК-3
44.	a	Какое направление совершенствования инфраструктуры управления ключами является наиболее актуальным для промышленных КФС согласно межгосударственному стандарту ГОСТ 34.10-2018? **a) Строгое разделение процессов генерации параметров схемы цифровой подписи субъектами схемы.**	ПК-3

		b) Использование единых параметров для всех субъектов без исключений. c) Отказ от стандартизации процесса генерации ключей. d) Генерация ключей на несертифицированном оборудовании.	
45.	a	Какое усовершенствование протоколов аутентификации и подписи необходимо для интеграции с Zero Trust архитектурой в КФС? **a) Внедрение расширенной аутентификации устройств с использованием цифровых сертификатов и безопасного обмена ключами на старте сеанса.** b) Отказ от взаимной аутентификации компонентов. c) Использование общего пароля для всех сервисов внутри доверенной зоны. d) Отключение проверки подлинности для внутреннего трафика.	ПК-3
46.	a	Какое решение предлагается для ретроспективной модернизации аутентификации в существующих морских системах (SIGMAR)? **a) Недорогое решение для «ретрофита» аутентификации навигационных данных на основе асимметричной криптографии.** b) Полная замена всего навигационного оборудования. c) Отказ от аутентификации навигационных данных. d) Использование только бумажных карт и визуального контроля	ПК-3
47.	a	Какую проблему решает интеграция децентрализованных схем подписи на основе атрибутов (DMA-ABS) в КФС? **a) Обеспечение эффективной и безопасной подписи в средах с несколькими центрами полномочий.** b) Упрощение структуры ключей до одного центрального удостоверяющего центра. c) Отказ от проверки атрибутов подписанта. d) Снижение общего уровня безопасности системы.	ПК-3
48.	a	Какое усовершенствование процесса управления документами обеспечивает использование детерминированной электронной подписи?	ПК-3

		a) Возможность использования подписи в качестве контрольной суммы и облегчение управления документами. b) Невозможность проверить подлинность подписи. c) Зависимость подписи от случайных чисел, генерируемых при каждом подписании. d) Отсутствие привязки подписи к содержимому документа.	
49.	a	Какое направление совершенствования СУИБ КФС наиболее полно соответствует переходу от реактивной к проактивной защите? a) Внедрение активного мониторинга, обеспечивающего своевременную информированность методов управления безопасностью. b) Проведение аудита безопасности раз в несколько лет. c) Реагирование на инциденты только после наступления ущерба. d) Полный отказ от мониторинга безопасности в пользу физической защиты.	ПК-3
50.	b	В чем заключается специфика контекстно-зависимой аутентификации для КФС (например, для интеллектуальных транспортных систем)? a) Аутентификация выполняется только один раз при запуске устройства. b) Аутентификация усиливается за счет привязки цифровых учетных данных к физическим факторам, таким как местоположение и время. c) Она не требует проверки личности пользователя. d) Она основана только на анализе трафика сети.	ПК-3

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, 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
- дополняет свой ответ информацией из дополнительных источников;
- в своей речи использует в полном объеме специальные термины;
- ответ логичен и последователен;
- выводы аргументированы и доказательны.

Оценка «хорошо» выставляется студенту, если
- демонстрирует хорошее владение учебной информацией, определенной рамками учебной дисциплины;
- демонстрирует достаточные знания, владеет специальной терминологией;
- ответ на поставленный вопрос излагается систематизировано и последовательно, при этом допускает определенные неточности в подаче материала.

Оценка «удовлетворительно» выставляется студенту, если
- в процессе ответа на вопрос допускает нарушение в последовательности изложения материала;
- неточно употребляет специальные термины;
- не делает выводы по изложенному материалу (поверхностный характер ответа).

Оценка «неудовлетворительно» выставляется студенту, если
- отвечая на вопросы не последователен, не логичен;
- не демонстрирует определенные системы знаний по предмету;
- не владеет основной и дополнительной литературой, не делает выводы;
- не владеет понятийным аппаратом по данной дисциплине.