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

Технологии доверенного взаимодействия киберфизических систем

Направление подготовки	10.04.01 Информационная безопасность
Направленность (профиль)	Информационная безопасность киберфизических систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	1

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 «Технологии доверенного взаимодействия киберфизических систем».

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

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 «Технологии доверенного взаимодействия киберфизических систем».

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 (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Высокий уровень (отлично) 5 баллов
ПК-2 Способен проектировать и реализовывать политику безопасности вычислительных сетей в киберфизических системах				
ПК-2 ИД-2 проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах	на низком уровне проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах	в основном проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах	умеет проектировать и реализовать политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне проектирует и реализует политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-3 комплекс выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на низком уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	в основном владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном уровне владеет навыками реализации комплекса выбранных мер, при реализации политики безопасности вычислительных сетей в киберфизических системах
ПК-2 ИД-4 формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	на низком уровне формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	в основном формализует результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	может формализовать результаты проектирования и реализацию политики безопасности вычислительных сетей в киберфизических системах	на высоком профессиональном 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 функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	на низком уровне: знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	в основном знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	знает состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне знает 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-5 реализует технологии разработки предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	на низком уровне реализует технологии разработки предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	в основном реализует технологии разработки предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	может реализовать технологии разработки предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	на высоком профессиональном уровне реализует технологии разработки предложений по совершенствованию системы управления информационной безопасностью 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 1	
1.	b	Какой стандарт регламентирует профили защиты для промышленных систем автоматизации и управления? a) ISO 27001 b) **IEC 62443** c) ГОСТ Р 56545 d) IEEE 802.11	ПК-2
2.	a	Какой компонент используется для хранения измерений состояния системы при доверенной загрузке? a) **PCR (Platform Configuration Registers) внутри TPM** b) CMOS-память c) Буфер обмена d) Виртуальная память	ПК-2
3.	b	Что такое «анклав» (enclave) в технологии Intel SGX? a) Среда исполнения с полным доступом ко всей памяти b) **Изолированная область памяти и процессора, защищённая от ОС и гипервизора** c) Специальный драйвер для USB d) Аппаратный генератор случайных чисел	ПК-2
4.	b	Какой метод привязки использует уникальный серийный номер процессора для лицензирования ПО? a) Хеширование файла лицензии b) **Создание ключа привязки на основе данных CPUID и TPM** c) Проверка MAC-адреса через ARP d) Запись в реестр Windows	ПК-2
5.	b	Какой алгоритм чаще всего используется для вычисления MAC в протоколах промышленных сетей? a) MD2	ПК-2

		b) **HMAC-SHA256** c) RC4 d) Base64	
6.	c	Что обеспечивает цифровая подпись в дополнение к целостности? a) Конфиденциальность b) Сжатие c) **Неотказуемость (non-repudiation)** d) Анонимность	ПК-2
7.	b	Какой протокол используется для централизованной аутентификации устройств по технологии 802.1X? a) SNMP b) **RADIUS** c) ICMP d) BGP	ПК-2
8.	b	Какой объект PKI содержит открытый ключ и подпись удостоверяющего центра? a) CRL b) **Сертификат X.509** c) CSR d) Закрытый ключ	ПК-2
9.	b	Какая процедура выполняется для создания пары «закрытый – открытый ключ» в защищённом исполнении? a) Импорт ключа с флешки b) **Генерация ключей непосредственно на устройстве с использованием TPM/HSM** c) Запрос ключа по электронной почте d) Копирование из реестра Windows	ПК-2
10.	b	Какой RFC описывает форматы сертификатов и списков отзыва CRL в инфраструктуре PKIX? a) RFC 1035 b) **RFC 5280** c) RFC 791 d) RFC 2131	ПК-2

11.	b	Какой формат используется для зашифрованного транспорта закрытого ключа и сертификата (например, для обмена между устройствами)? a) PEM b) **PKCS#12 (PFX)** c) DER d) XML	ПК-2
12.	a	Какой компонент УЦ отвечает за регистрацию и проверку личности заявителя перед выпуском сертификата? a) **Регистрационный центр (RA)** b) Валидатор OCSP c) Хранилище меток времени d) Сетевой шлюз	ПК-2
13.	b	Какое условие обязательно для придания юридической силы документу, подписанному в КФС, на территории РФ? a) Использование простой электронной подписи b) **Наличие усиленной квалифицированной электронной подписи и сертификата аккредитованного УЦ** c) Отправка документа по факсу d) Нотариальное заверение	ПК-2
14.	a	Какой тип атаки позволяет злоумышленнику выдать поддельный сертификат, если скомпрометирован корневой ключ УЦ? a) **Подмена корневого сертификата и выпуск ложных сертификатов** b) DDoS на OCSP-респондер c) Перехват сессии TLS d) Подбор пароля пользователя	ПК-2
15.	b	Какое средство обязательно для защиты закрытых ключей удостоверяющего центра? a) Антивирус Касперского b) **Аппаратный модуль безопасности (HSM) с контролем доступа** c) Облачное хранилище с двухфакторной аутентификацией d) Резервное копирование на USB-накопитель	ПК-2
16.	b	В чём заключалась основная новация системы Secure Electronic Transaction (SET) для платёжных карт?	ПК-2

		a) Использование только симметричного шифрования b) **Применение двойной цифровой подписи для разделения платёжной информации и данных заказа** c) Отказ от сертификатов d) Передача PIN-кода в открытом виде	
17.	b	Какой принцип является основным для архитектуры Zero Trust в КФС? a) Доверять всем устройствам внутри периметра b) **Никогда не доверять, всегда проверять (never trust, always verify)** c) Доверять только после одноразовой аутентификации d) Доверять на основе IP-адреса	ПК-2
18.	b	Какое техническое ограничение чаще всего применяется для BYOD-устройств при доступе к сети КФС? a) Предоставление полных прав администратора b) **Изоляция в отдельный сегмент сети (VLAN) и запрет прямого доступа к контроллерам** c) Отключение всех средств шифрования d) Использование только открытых Wi-Fi сетей	ПК-2
19.	a	Какой стандарт определяет требования к системе менеджмента информационной безопасности (СМИБ) в общем виде? a) **ISO/IEC 27001** b) IEC 62351 c) NIST SP 800-82 d) IEEE 1588	ПК-2
20.	b	Какая технология позволяет удалённо проверить, что на узле КФС загружено доверенное ПО? a) Secure Boot b) **Remote Attestation (удалённая аттестация) на основе TPM** c) UEFI BIOS d) Антивирусное сканирование	ПК-2
21.	b	Как называется механизм, при котором программное обеспечение может выполняться только при наличии физически подключённого USB-токена с лицензией? a) Обфускация кода	ПК-2

		b) **Аппаратный донгл (Hardware Dongle)** c) Виртуализация лицензии d) Облачная активация	
22.	a	Какой протокол обеспечивает защиту от подмены ARP-таблиц в локальной сети КФС? a) **DAI (Dynamic ARP Inspection)** b) STP c) VRRP d) SNMPv3	ПК-2
23.	b	Какой стандарт описывает EAP (Extensible Authentication Protocol) для беспроводных сетей? a) IEEE 802.3 b) **IEEE 802.1X** c) IEEE 802.11ac d) IEEE 802.15.4	ПК-2
24.	b	Как называется процесс смены ключей шифрования в сеансе связи без разрыва соединения? a) Регистрация ключа b) **Ротация ключей (key rotation)** c) Депонирование ключа d) Аннулирование ключа	ПК-2
25.	c	Какой структура данных PKI содержит перечень серийных номеров отозванных сертификатов? a) CSR b) OCSP-ответ c) **CRL (Certificate Revocation List)** d) PKCS#7	ПК-3
26.	b	Какая уязвимость в PKI наиболее критична для КФС с длительным сроком жизни (10+ лет)? a) Отсутствие резервного копирования b) **Использование устаревших хеш-алгоритмов (например, SHA-1) в корневых сертификатах**	ПК-3

		c) Слишком частый выпуск CRL d) Большой размер сертификатов	
27.	b	Какое усовершенствование процедуры проверки сертификатов повышает безопасность при компрометации OCSP-респондера? a) Отказ от проверки статуса b) **Внедрение мультипатчной проверки (multiple OCSP responders с консенсусом)** c) Увеличение времени кэширования d) Использование только CRL	ПК-3
28.	b	Какое дополнение к протоколам промышленной автоматизации (Modbus, DNP3) эффективно защищает от модификации команд? a) Добавление контрольной суммы CRC16 b) **Внедрение цифровой подписи каждого кадра с временной меткой** c) Передача команд в открытом виде d) Отключение аутентификации	ПК-3
29.	b	Какая стратегия управления ключами рекомендуется для КФС с децентрализованной топологией (например, сеть датчиков)? a) Единый ключ для всех устройств b) **Гибридная схема с предварительным распределением ключей и их периодической ротацией через защищённый канал** c) Хранение ключей в открытом виде в ПЗУ d) Отказ от шифрования	ПК-3
30.	b	Какой компонент необходимо добавить в существующую КФС для перехода к модели Zero Trust? a) Один общий VPN-сервер b) **Микросегментация с контролем каждого потока данных и политиками на основе идентичности** c) Увеличение числа межсетевых экранов на периметре d) Полное отключение аутентификации	ПК-3
31.	b	Какое организационное решение повышает безопасность BYOD в КФС? a) Запрет любых личных устройств b) **Внедрение контейнеризации приложений и обязательной аттестации устройства перед подключением**	ПК-3

		c) Использование одинакового пароля для всех d) Отключение журналирования	
32.	b	Какой тип атак на TPM может привести к раскрытию ключей и требует совершенствования аппаратной защиты? a) DDoS b) **Атаки по сторонним каналам (power analysis, timing attacks)** c) Фишинг d) Подбор пароля BIOS	ПК-3
33.	b	Какое нововведение повышает долговременную юридическую силу подписей в КФС (на десятки лет)? a) Использование коротких сертификатов (1 день) b) **Применение технологии LTV (Long-Term Validation) с добавлением меток времени и доказательств валидности** c) Отказ от квалифицированной подписи d) Хранение подписей на бумаге	ПК-3
34.	b	Какое расширение протокола OCSP снижает нагрузку на УЦ и повышает конфиденциальность? a) OCSP без подписи b) **OCSP Stapling (сервер сам прикрепляет подписанный OCSP-ответ)** c) OCSP через HTTP d) Отключение OCSP	ПК-3
35.	b	Какой метод повышает защиту от аутентификации с подменой узла в сетях LoRaWAN? a) Использование фиксированного DevAddr b) **Применение динамического сеансового ключа с подтверждением на уровне приложения** c) Передача ключа в открытом виде d) Отказ от шифрования	ПК-3
36.	b	Какая практика улучшает доверие к прошивкам встроенных систем в КФС? a) Отказ от цифровой подписи прошивок b) **Двухэтапное обновление с проверкой подписи и обязательной перезагрузкой в защищённом режиме**	ПК-3

		c) Обновление по открытому FTP d) Использование одинаковой прошивки для всех устройств	
37.	b	Какой современный подход позволяет привязать приложение к виртуальной машине в облаке без TPM? a) Использование статического пароля b) **Виртуальный TPM (vTPM) с измерением гипервизора** c) Запись лицензии в файл d) Проверка по IP-адресу	ПК-3
38.	b	Какой недостаток системы SET был устранён в современных протоколах (например, 3D Secure 2.0)? a) Низкая скорость работы b) **Сложность внедрения и необходимость установки специального ПО на клиентской стороне** c) Отсутствие шифрования d) Несовместимость с картами Visa	ПК-3
39.	b	Какая технология автоматизации PKI наиболее подходит для КФС с 10 000+ узлов? a) Ручной выпуск сертификатов b) **Протокол EST (Enrollment over Secure Transport) с автоматическим продлением** c) Передача сертификатов через флешки d) Использование самоподписанных сертификатов без УЦ	ПК-3
40.	b	Какой метод помогает обнаружить попытку компрометации администратора УЦ? a) Ежедневная смена пароля b) **Анализ поведения (UEBA) с контролем нештатных операций выдачи сертификатов** c) Отключение аудита d) Предоставление прав всем сотрудникам	ПК-3
41.	b	Какой протокол рекомендуется для аутентификации в сетях с частыми обрывами связи (например, спутниковые КФС)? a) Kerberos b) **Протокол с сохранением состояния и повторной аутентификацией на основе ключей сессии**	ПК-3

		c) Одноразовые пароли по SMS d) Аутентификация по MAC-адресу	
42.	b	Какое дополнение к IEC 62443 необходимо для учёта постквантовых угроз? a) Запрет на использование криптографии b) **Включение рекомендаций по миграции на постквантовые алгоритмы для систем с длительным жизненным циклом** c) Увеличение длины паролей до 30 символов d) Отказ от аутентификации	ПК-3
43.	b	Какую функцию следует добавить в TPM следующего поколения для КФС? a) Встроенный Wi-Fi b) **Поддержка постквантовых алгоритмов на аппаратном уровне** c) Увеличение тактовой частоты d) RGB-подсветка	ПК-3
44.	b	Какой метод обеспечивает защиту от модификации данных при передаче через последовательный интерфейс RS-485 в устаревших КФС? a) Контроль по чётности b) **Внешний криптографический шлюз, вычисляющий MAC и вставляющий его в зарезервированные поля кадра** c) Отказ от передачи данных d) Удвоение каждого байта	ПК-3
45.	b	Какая архитектура объединяет BYOD и Zero Trust для КФС? a) Все устройства получают полный доступ b) **Каждое BYOD-устройство проходит непрерывную аттестацию, а доступ предоставляется только к конкретным функциям на основе политик** c) Использование общего пароля d) Отключение логирования	ПК-3
46.	b	Какой способ распространения CRL наиболее эффективен для крупной КФС с медленными каналами связи? a) Рассылка полного CRL каждому узлу ежечасно b) **Использование дельта-CRL (delta CRL) с отправкой только изменений** c) Отказ от CRL d) Публикация CRL в газете	ПК-3

47.	b	Какое требование необходимо для взаимного признания электронных подписей в КФС разных стран? a) Использование национальных стандартов без согласования b) **Гармонизация нормативной базы и применение стандартов, рекомендованных международными организациями (например, ЕАЭС)** c) Отказ от подписей d) Обязательный нотариус	ПК-3
48.	b	Какая схема подписи наиболее легковесна для устройств класса 8-битных микроконтроллеров? a) RSA-2048 b) **ECDSA на эллиптической кривой (например, secp256r1) с аппаратным ускорителем** c) ГОСТ 34.10-2012 d) Подпись на основе MD5	ПК-3
49.	b	Какая технология позволяет отказаться от единого УЦ в распределённой КФС? a) Статические ключи в ПЗУ b) **Децентрализованная PKI на основе блокчейна (например, смарт-контракты для записи сертификатов)** c) Отсутствие сертификатов d) Центральный сервер с паролями	ПК-3
50.	b	Какой показатель (метрика) должна быть добавлена в СУИБ КФС для оценки эффективности аутентификации? a) Количество выданных паролей b) **Время обнаружения и блокировки аномального узла (MTTD и MTTB)** c) Скорость передачи данных d) Количество подключённых устройств	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.

** в соответствии с результатами освоения дисциплины*