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

УТВЕРЖДАЮ
И.о. директора института перспективной инженерии
_____ А.А.Порохня

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

Кибербезопасность

Направление подготовки	09.03.04 Программная инженерия
Направленность (профиль)	Инженерия сложных программных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в	8 семестре

Введение

1. Назначение: Оценочные материалы (оценочные средства) предназначены для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, и представляют собой совокупность контрольно-измерительных материалов и методов их использования для измерения уровня достижения обучающимся установленных результатов обучения.

2. ФОС является приложением к программе дисциплины «Кибербезопасность».

3. Разработчик Потапов И.Р., ассистент межинститутской базовой кафедры департамента цифровых, робототехнических систем и электроники

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Новикова Елена Николаевна, зав. межинститутской базовой кафедрой

(ФИО, должность)

Члены комиссии:

Николаев Евгений Иванович, доцент департаменты цифровых и робототехнических систем и электроники.

(ФИО, должность)

Винокурский Д. Л., доцент департамента цифровых, робототехнических систем и электроники

(ФИО, должность)

Представитель организации-работодателя: А. В. Новиков, начальник отдела АСУТП ООО «ЕНДС-Ставрополь»

(ФИО, должность)

Экспертное заключение: Оценочные материалы (оценочные средства) по дисциплине «Кибербезопасность» составлены в соответствии с требованиями самостоятельно устанавливаемого Федерального государственного образовательного стандарта высшего образования по направлению 09.03.04 «Программная инженерия» и позволяют оценить уровень сформированности компетенции ПК-10.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

.

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

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: **ПК-10** – Готов соблюдать правовые нормы, стандарты и требования информационной безопасности, участвовать в разработке нормативной и технической документации, учитывать законодательство в области ИТ				
Результаты обучения по дисциплине (модулю): *Индикатор:* ПК-$10_{ИД-1}$ – Применяет основные правовые нормы (лицензирование ПО, авторское право, ФЗ-152, ФЗ-149) и стандарты ИБ (ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 56545-2015) при разработке и эксплуатации ПО	Не знает ФЗ-152, ФЗ-149, ГОСТ 27001; не может описать процедуру реагирования на инцидент	Знает названия основных законов (ФЗ-152, ФЗ-149) и стандарта ИСО 27001, но не может применить их к конкретной ситуации	Приводит примеры требований к обработке персональных данных (ФЗ-152), описывает базовую процедуру реагирования (обнаружение → локализация → устранение → анализ)	Полноценно применяет нормативные требования при разработке ПО (согласие на обработку ПДн, уведомление регулятора), составляет схему управления инцидентами в соответствии с ГОСТ Р 56545-2015, заполняет журнал инцидентов
Результаты обучения по дисциплине (модулю): *Индикатор:* ПК-$10_{ИД-2}$ – Реализует меры защиты информации: аутентификацию (JWT, OAuth2), авторизацию (RBAC), шифрование, защиту от типовых уязвимостей OWASP Top 10 (SQL-инъекции, XSS, CSRF, IDOR) с учётом требований регуляторов (ФСТЭК)	Не умеет проводить пентест, не знает OWASP Top 10, не оформляет отчёты	Проводит простой сканер-пентест (например, OWASP ZAP в автоматическом режиме), выводит список уязвимостей без контекста, отчёт не структурирован	Применяет стандартные чек-листы OWASP для ручной проверки XSS, SQLi, IDOR; оформляет акт о пентесте с перечислением найденных уязвимостей и ссылками на CWE	Проводит полноценный пентест с использованием методологии PTES или OWASP, оформляет детальный отчёт (риски по CVSS, доказательства, рекомендации по исправлению), прилагает акт о соответствии требованиям регулятора (ФСТЭК, если необходимо)
Результаты обучения по дисциплине (модулю):	Не умеет разрабатывать	Составляет простую	Разрабатывает модель угроз	Полный комплект: политика

Индикатор: ПК-10$_{ИД-3}$ – Разрабатывает нормативную и техническую документацию по информационной безопасности: политики парольной защиты, модели угроз, технические задания на подсистему ИБ, инструкции пользователя, регламенты реагирования на инциденты	документацию по ИБ, не знает структуры модели угроз	парольную политику (длина, сложность) на одной странице, без модели угроз	для небольшой системы (источники, типы угроз, базовый уровень защищённости), составляет ТЗ на подсистему ИБ (2–3 требования), пишет инструкцию пользователя по безопасной работе	парольной защиты и управления доступом, модель угроз по методике ФСТЭК (с активами, угрозами, нарушителями), ТЗ на подсистему ИБ с функциональными требованиями, регламент реагирования на инциденты (этапы, роли, сроки), инструкции пользователя и администратора, акт оценки соответствия требованиям кибербезопасности

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1.	2	Какой документ согласно законодательству РФ (Приказ ФСТЭК № 239) определяет порядок действий при обнаружении инцидентов информационной безопасности? 1) Политика обработки персональных данных 2) Регламент реагирования на инциденты ИБ 3) Техническое задание на разработку ПО 4) Договор на оказание услуг	ПК-10
2.	1,3	Какие из перечисленных нормативных актов регулируют обработку персональных данных в РФ? (Выберите все верные) 1) Федеральный закон № 152-ФЗ «О персональных данных» 2) ГОСТ Р ИСО/МЭК 27001 3) Приказ ФСТЭК № 21 (об утверждении состава и содержания мер по защите ПД) 4) Уголовный кодекс (в части киберпреступлений)	ПК-10
3.	3	Что такое CVSS (Common Vulnerability Scoring System)? 1) База данных уязвимостей 2) Стандарт шифрования 3) Система оценки критичности уязвимостей (базовые, временные, экологические метрики) 4) Протокол безопасной передачи данных	ПК-10
4.	2	Какой стандарт международной серии ISO/IEC 27000 описывает требования к системе менеджмента информационной безопасности (СМИБ)? 1) ISO/IEC 27002 2) ISO/IEC 27001 3) ISO/IEC 27005 4) ISO 9001	ПК-10
5.	4	Что из перечисленного является обязательным элементом договора на проведение тестирования на проникновение (пентеста) с правовой точки зрения? 1) Список использованных инструментов	ПК-10

		2) Технический отчёт о найденных уязвимостях 3) Справка о доходах исполнителя 4) Письменное разрешение от владельца системы (включая границы тестирования и правила взаимодействия)	
6.	2	Какой орган в РФ осуществляет регулирование в области защиты государственной тайны и сертификации средств защиты информации? 1) Министерство цифрового развития 2) ФСТЭК России 3) Роскомнадзор 4) МВД	ПК-10
7.	3	Какой раздел должен быть обязательно включён в план непрерывности бизнеса (BCP) в соответствии с требованиями регуляторов? 1) Маркетинговый бюджет 2) Штатное расписание 3) Порядок резервного копирования и восстановления критически важных данных, с указанием RTO и RPO 4) Описание корпоративной культуры	ПК-10
8.	1	Что означает аббревиатура RTO в документации по восстановлению после сбоя (DRP)? 1) Recovery Time Objective (целевое время восстановления) – максимальное допустимое время простоя системы 2) Recovery Point Objective (целевая точка восстановления) 3) Return to Operation 4) Real Time Operations	ПК-10
9.	4	Какой этап жизненного цикла уязвимости (согласно стандартам) включает публикацию CVE-идентификатора и описание в NVD? 1) Обнаружение внутри организации 2) Эксплуатация в реальных атаках 3) Разработка патча 4) Раскрытие информации (Disclosure)	ПК-10
10.	2	Какие требования к сроку хранения логов событий ИБ обычно устанавливаются для операторов персональных данных (ФЗ-152)? 1) Не менее 6 месяцев	ПК-10

		2) Не менее 1 года (или в соответствии с внутренними актами, но часто 1–3 года) 3) Не менее 5 лет 4) Не регламентируется	
11.	3	Что из перечисленного относится к категории «нормативно-технической документации» в области информационной безопасности? 1) Презентация для инвесторов 2) Заявление о приеме на работу 3) Политика безопасности, регламент реагирования на инциденты, инструкция пользователя по ИБ 4) Технический паспорт на оборудование	ПК-10
12.	1,4	Какие действия необходимо выполнить при оформлении акта тестирования на проникновение для соблюдения правовых норм? (Выберите все верные) 1) Указать даты, время и объем тестирования 2) Опубликовать акт в открытом доступе 3) Приложить исходные коды эксплойтов 4) Получить утверждение акта у руководства организации-заказчика	ПК-10
13.	2	Какой стандарт описывает процесс управления инцидентами информационной безопасности (в частности, этапы подготовки, обнаружения, сдерживания, эрадикации, восстановления)? 1) ISO 22301 (BCM) 2) NIST SP 800-61 (Computer Security Incident Handling Guide) 3) PCI DSS 4) GDPR	ПК-10
14.	3	В соответствии с каким нормативным документом в РФ операторы КИИ обязаны сообщать об инцидентах в ГосСОПКА? 1) ФЗ-149 «Об информации...» 2) ФЗ-187 «О безопасности КИИ РФ» 3) Постановление Правительства № 127 (о порядке информирования) 4) Указ Президента № 000	ПК-10
15.	4	Что такое «модель угроз» с точки зрения требований ФСТЭК (для систем обработки персональных данных)? 1) Перечень известных компьютерных атак 2) Описание архитектуры сети	ПК-10

		3) Результаты пентеста 4) Документированный перечень актуальных угроз, вероятных источников и способов их реализации применительно к конкретной системе	
16.	2	Какой из перечисленных документов требуется при внедрении SIEM-системы для соблюдения регуляторных требований? 1) Лицензия на программное обеспечение 2) Политика сбора и хранения событий ИБ (с указанием сроков, состава событий, прав доступа к логам) 3) Справка об отсутствии судимости у администратора 4) Паспорт сервера	ПК-10
17.	1	Какая ответственность предусмотрена Уголовным кодексом РФ за неправомерный доступ к компьютерной информации (ст. 272)? 1) Штраф, исправительные работы, либо лишение свободы до 2 лет (в зависимости от тяжести) 2) Только дисциплинарная ответственность 3) Административный штраф до 5000 руб. 4) Выговор	ПК-10
18.	3	Что должно быть указано в техническом задании на проведение работ по анализу защищённости для соблюдения правовых норм? 1) Пожелания заказчика по интерфейсу отчёта 2) Стоимость часа работы специалиста 3) Границы тестирования, разрешённые методы, сроки, порядок предоставления отчёта, ответственность сторон 4) Резюме исполнителей	ПК-10
19.	2	Какой международный стандарт регламентирует управление рисками информационной безопасности? 1) ISO 9001 2) ISO/IEC 27005 3) ISO 14001 4) OWASP ASVS	ПК-10
20.	4	Какие сведения НЕ подлежат разглашению в публичном отчёте о пентесте (согласно этике и законодательству)? 1) Общее количество найденных уязвимостей	ПК-10

		2) Используемые методологии 3) Дата проведения теста 4) Детальные технические описания уязвимостей и способы их эксплуатации	
21.	1	Что из перечисленного является обязательной частью плана реагирования на инциденты (IRP) в соответствии с рекомендациями ФСТЭК? 1) Список членов группы реагирования (CSIRT/CERT) с контактами и ролями 2) Бизнес-план организации 3) Описание праздничных дней 4) Программа мотивации сотрудников	ПК-10
22.	3	Какие требования к резервному копированию содержатся в ФЗ-152 для операторов ПД? 1) Резервное копирование не требуется 2) Копии должны храниться только на бумаге 3) Должны быть обеспечены восстановление и возможность контроля целостности копий (согласно актуальным нормативным актам) 4) Копии должны быть зашифрованы, но сроки не указаны	ПК-10
23.	2	Что такое «Compliance as Code» в DevSecOps? 1) Автоматическая генерация лицензий 2) Представление нормативных требований в виде машинно-читаемых правил (например, Rego, OPA), проверяемых в CI/CD пайплайне 3) Ручная проверка compliance-инженером 4) Отказ от комплаенса	ПК-10
24.	1,4	Какие из перечисленных действий являются правомерными при проведении тестирования на проникновение? (Выберите все верные) 1) Получение письменного разрешения от заказчика с указанием границ 2) Использование вредоносного ПО без предупреждения 3) Атака на системы третьих лиц, затронутые в ходе теста 4) Подписание договора о неразглашении (NDA) между сторонами	ПК-10
25.	3	Какой документ регламентирует порядок классификации инцидентов ИБ в государственных системах РФ? 1) Методика оценки рисков ЦБ РФ 2) Приказ ФАС	ПК-10

		3) Приказ ФСТЭК № 31 (или аналогичный, определяющий категорирование инцидентов) 4) СанПиН	
26.	2	Что из перечисленного является нарушением законодательства РФ при организации мониторинга сотрудников? 1) Уведомление сотрудников о мониторинге в трудовом договоре 2) Скрытый сбор логинов и паролей сотрудников без их согласия (вне служебных заданий) 3) Запись рабочего времени через систему контроля доступа 4) Анализ корпоративной переписки при расследовании инцидента с согласия	ПК-10
27.	1	Какая информация должна быть отражена в акте проверки системы защиты информации (СЗИ) по результатам аттестации объекта информатизации? 1) Перечень реализованных мер, выявленные несоответствия требованиям, заключение о соответствии, подписи комиссии 2) Количество установленных антивирусов 3) Список сотрудников, имеющих доступ 4) Реквизиты банковского счёта	ПК-10
28.	4	Согласно ФЗ-149 «Об информации…», что является обязательным требованием к хранению данных граждан РФ? 1) Данные должны храниться только на бумаге 2) Данные должны быть зашифрованы российскими сертифицированными средствами 3) Данные должны храниться не менее 10 лет 4) Персональные данные граждан РФ должны храниться на серверах, расположенных на территории РФ	ПК-10
29.	2	Какой документ определяет перечень сведений, составляющих государственную тайну, в Российской Федерации? 1) Уголовный кодекс 2) Закон РФ «О государственной тайне» (в частности, статьи и перечни) 3) Трудовой кодекс 4) Конституция РФ	ПК-10
30.	3	Какие требования предъявляются к документации по защите информации для объектов КИИ (критической информационной инфраструктуры)?	ПК-10

		1) Документация не требуется 2) Документация может быть в свободной форме 3) Разработка и утверждение организационно-распорядительных документов (политик, планов) в соответствии с приказами ФСТЭК (например, № 239) 4) Только технический паспорт	
31.	1	Как часто должен пересматриваться план непрерывности бизнеса (BCP) согласно лучшим практикам (ISO 22301) и рекомендациям Банка России? 1) Не реже одного раза в год, а также после крупных изменений или инцидентов 2) Один раз в 5 лет 3) Никогда, если всё работает 4) Только по требованию прокуратуры	ПК-10
32.	4	Какие данные должны быть зафиксированы в журнале регистрации событий безопасности SIEM для соответствия требованиям регулятора (например, ФСТЭК)? 1) Только IP-адреса 2) Только дата и время 3) Только пользователь 4) Дата, время, субъект доступа, объект доступа, результат действия, идентификатор события	ПК-10
33.	2	Что из перечисленного является обязанностью оператора персональных данных согласно ст. 18.1 ФЗ-152? 1) Публиковать все персональные данные в открытых источниках 2) Назначить ответственного за обработку ПД и утвердить политику в отношении обработки ПД 3) Передать все данные в ФСБ 4) Уничтожить данные через месяц после сбора	ПК-10
34.	3	Какие требования предъявляются к использованию средств криптографической защиты информации (СКЗИ) для защиты ПД в государственных информационных системах? 1) Можно использовать любые бесплатные программы 2) Обязательно сертифицированное ФСТЭК/ФСБ СКЗИ и соблюдение правил эксплуатации (документация, ключевая документация) 3) Требования зависят от уровня защищённости ПД, но обычно требуется сертификация	ПК-10

		4) СКЗИ не требуются	
35.	2	Какой нормативный акт регулирует порядок уведомления об утечках персональных данных в Роскомнадзор? 1) Федеральный закон «О рекламе» 2) Приказ Роскомнадзора о форме уведомления (на основании ч. 3.1 ст. 21 ФЗ-152) 3) Постановление Правительства о лицензировании 4) Инструкция ЦБ РФ	ПК-10
36.	2	Какой регламентирующий документ в РФ устанавливает порядок проведения классификации информационных систем персональных данных (ИСПДн)? 1) ФЗ-149 2) Приказ ФСТЭК № 21 (утверждает состав и содержание организационных и технических мер по защите ПД) 3) СанПиН 2.2.4 4) ГОСТ Р 34.10	ПК-10
37.	1,3	Какие из перечисленных документов являются обязательными для оператора персональных данных (ФЗ-152)? (Выберите все верные) 1) Политика в отношении обработки персональных данных 2) Справка о доходах сотрудника 3) Перечень мер по обеспечению безопасности ПД 4) Штатное расписание	ПК-10
38.	4	Какое наказание предусмотрено КоАП РФ за нарушение установленного порядка обработки персональных данных (для должностных лиц)? 1) Уголовный срок до 5 лет 2) Только предупреждение 3) Дисквалификация до 1 года 4) Штраф от 10 000 до 100 000 рублей (в зависимости от статьи и тяжести)	ПК-10
39.	2	В каком случае оператор ПД вправе отказать субъекту ПД в доступе к его персональным данным? 1) Если данные хранятся в облаке за пределами РФ 2) Если предоставление доступа нарушает права и законные интересы третьих лиц (ст. 14 ФЗ-152) 3) Если субъект ПД не указал свой паспорт	ПК-10

		4) Никогда, доступ должен быть предоставлен всегда	
40.	3	Какой международный стандарт описывает требования к безопасности платёжных карт (индустрия пластиковых карт)? 1) ISO 27001 2) HIPAA 3) PCI DSS (Payment Card Industry Data Security Standard) 4) SOX	ПК-10
41.	1	Что из перечисленного является обязательным требованием PCI DSS для хранения данных о держателях карт? 1) Запрет на хранение кода аутентификации (CVV/CVC) после авторизации 2) Хранение CVV в открытом виде для ускорения платежей 3) Передача пана по электронной почте 4) Отсутствие шифрования	ПК-10
42.	4	Какие данные о платёжных картах разрешается хранить при соблюдении PCI DSS? 1) Полный номер карты (PAN), срок действия, имя держателя (при шифровании) 2) CVV/CVC 3) Пин-код 4) Только последние 4 цифры пана, и то с ограничениями (PAN в зашифрованном виде при необходимости)	ПК-10
43.	2	Что такое GDPR (General Data Protection Regulation) и на кого распространяется? 1) Российский закон о персональных данных 2) Регламент ЕС о защите данных, распространяющийся на любые организации, обрабатывающие данные граждан ЕС, независимо от местонахождения 3) Стандарт криптографии 4) Протокол безопасной передачи	ПК-10
44.	3,4	Какие права субъекта данных вводит GDPR, отсутствовавшие в старой Директиве ЕС? (Выберите все верные) 1) Право на забвение (право на удаление) 2) Право на переносимость данных 3) Право на ограничение обработки 4) Право не подвергаться автоматизированному принятию решений, включая профилирование	ПК-10

45.	1	Какой срок уведомления надзорного органа об утечке персональных данных установлен в GDPR? 1) Не позднее 72 часов после обнаружения инцидента 2) 30 дней 3) Немедленно, но не позднее 24 часов 4) Не требуется уведомлять	ПК-10
46.	2	Что является обязательным требованием к согласию на обработку персональных данных по ФЗ-152? 1) Согласие может быть в устной форме в любом случае 2) Согласие должно быть конкретным, информированным, сознательным и может быть отозвано субъектом в любое время (в письменной форме) 3) Согласие действует бессрочно и не отзывается 4) Согласие не требуется, если данные уже собраны	ПК-10
47.	4	В каком нормативном акте РФ содержатся требования к использованию средств электронной подписи (ЭП)? 1) ФЗ-152 2) ФЗ-149 3) ФЗ-187 4) ФЗ-63 «Об электронной подписи»	ПК-10
48.	1	Какие виды электронной подписи различает ФЗ-63? 1) Простая электронная подпись, усиленная неквалифицированная, усиленная квалифицированная 2) Только простая и квалифицированная 3) Только цифровая и графическая 4) Односторонняя и двусторонняя	ПК-10
49.	3	Какое юридическое значение имеет усиленная квалифицированная электронная подпись (КЭП)? 1) Никакого 2) Приравнивается к простой подписи 3) Приравнивается к собственноручной подписи с печатью (в случаях, предусмотренных законом) 4) Требует нотариального заверения	ПК-10

50.	2	Какой орган в РФ выдает сертификаты ключей проверки квалифицированной электронной подписи? 1) ФСТЭК 2) Удостоверяющие центры, аккредитованные Минцифры 3) ФСБ 4) Роскомнадзор	ПК-10
51.	4	Что из перечисленного относится к организационным мерам защиты информации по ФЗ-152? 1) Использование криптошлюзов 2) Установка межсетевых экранов 3) Шифрование дисков 4) Назначение ответственного за обработку ПД и утверждение перечня лиц, имеющих доступ к ПД	ПК-10
52.	1	Какие требования к уничтожению персональных данных должны быть зафиксированы в документации оператора? 1) Порядок, способ и сроки уничтожения (в том числе акт об уничтожении) 2) Только порядок 3) Только сроки 4) Документация не требуется	ПК-10
53.	2,3	Какие из перечисленных сведений относятся к банковской тайне в РФ (ФЗ «О банках и банковской деятельности»)? (Выберите все верные) 1) ФИО клиента 2) Сведения о счетах и вкладах 3) Операции по счетам 4) Адрес проживания клиента	ПК-10
54.	3	Какой срок хранения сведений о фактах приёма-передачи электронных сообщений (метаданных) установлен для операторов связи согласно «пакету Яровой» (ФЗ-374)? 1) 6 месяцев 2) 1 год 3) До 3 лет (в зависимости от объёма, но требования постоянно ужесточаются) 4) Не хранить	ПК-10

55.	1	Что из перечисленного является нарушением при трансграничной передаче персональных данных? 1) Передача в страну, не входящую в «белый список» и без отдельного разрешения РКН 2) Передача в страну ЕС с согласия субъекта 3) Передача с уведомлением РКН 4) Передача в рамках контракта с субъектом	ПК-10
56.	4	Какой документ регламентирует порядок работы с инцидентами в критической информационной инфраструктуре (КИИ)? 1) ФЗ-152 2) ФЗ-149 3) Приказ ФСБ № 123 4) Приказ ФСТЭК № 239 (об утверждении Требований к обеспечению безопасности значимых объектов КИИ)	ПК-10
57.	2	Какой срок уведомления ФСТЭК об инциденте на объекте КИИ согласно Постановлению Правительства № 127? 1) Не позднее 12 часов 2) Не позднее 24 часов с момента обнаружения инцидента 3) Не позднее 72 часов 4) Не требуется	ПК-10
58.	3	Какие требования предъявляются к использованию иностранного программного обеспечения на объектах КИИ? 1) Запрещено любое иностранное ПО 2) Разрешено без ограничений 3) Запрещено использование после 2025 года (постановление № 1840), требуется импортозамещение, либо получение разрешения 4) Требуется обязательная сертификация ФСБ	ПК-10
59.	1,4	Какие организационные документы должны быть разработаны в организации для соблюдения требований ИБ (стандартный пакет)? (Выберите все верные) 1) Политика информационной безопасности 2) Технический паспорт здания 3) План эвакуации при пожаре 4) Регламент реагирования на инциденты	ПК-10

60.	2	Что такое «риск-аппетит» (risk appetite) в документации по управлению рисками ИБ? 1) Максимальный ущерб, который может получить организация 2) Уровень риска, который организация готова принять для достижения целей (документируется в стратегии управления рисками) 3) Вероятность наступления события 4) Стоимость устранения уязвимости	ПК-10
61.	3	Какой метод оценки рисков рекомендуется стандартом ISO/IEC 27005? 1) Только количественный 2) Только качественный 3) Комбинированный (качественный + количественный, например, матрица вероятности и ущерба) 4) Экспертный опрос без документации	ПК-10
62.	2	Какой документ должен быть подписан между оператором ПД и третьим лицом, осуществляющим обработку ПД по его поручению (субпроцессором)? 1) Лицензионный договор 2) Договор поручения (с перечнем операций, мер безопасности, обязательством о конфиденциальности) 3) Трудовой договор 4) Договор аренды	ПК-10
63.	4	Что из перечисленного является обязательным для включения в должностную инструкцию специалиста по ИБ? 1) План отпусков 2) График дежурств 3) Норма выработки 4) Обязанности по соблюдению режима конфиденциальности, порядка работы с защищаемой информацией и ответственность за нарушения	ПК-10
64.	1	Какие требования к лицензированию деятельности по технической защите конфиденциальной информации установлены в РФ? 1) Лицензия ФСТЭК (обязательное лицензирование) 2) Нотариальное заверение 3) Регистрация в Роскомнадзоре 4) Лицензия не требуется	ПК-10

65.	3	Какой документ определяет порядок аттестации объекта информатизации на соответствие требованиям информационной безопасности? 1) Политика ИБ 2) Технический регламент Таможенного союза 3) Руководящие документы ФСТЭК (например, «Автоматизированные системы. Защита от несанкционированного доступа. Классификация АС»)	ПК-10
66.	2	Что должно быть указано в предписании на проведение аттестации объекта информатизации? 1) Цена аттестации 2) Перечень проверяемых требований, методы контроля, сроки и состав аттестационной комиссии 3) Список кандидатур на увольнение 4) Результаты предыдущей проверки	ПК-10
67.	4	Какие из перечисленных категорий персональных данных являются специальными (требуют особого порядка обработки) по ФЗ-152? 1) ФИО и адрес 2) ИНН и СНИЛС 3) Игровые предпочтения 4) Раса, национальность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь	ПК-10
68.	1	В каком случае допускается обработка специальных категорий ПД без согласия субъекта? 1) Для установления пенсионного обеспечения, в случаях, предусмотренных законодательством 2) При любом желании оператора 3) Для рекламы 4) Для передачи третьим лицам в коммерческих целях	ПК-10
69.	3	Какой срок хранения документов, подтверждающих получение согласия на обработку ПД, установлен ФЗ-152? 1) Не менее 1 года 2) Не менее 2 лет 3) Не менее 3 лет (после прекращения обработки ПД) 4) Постоянно	ПК-10

70.	2	Что является нарушением порядка хранения биометрических персональных данных (отпечатки пальцев, изображение лица)? 1) Хранение в зашифрованном виде 2) Хранение вместе с иными персональными данными (без разделения) без отдельного согласия и без внесения в информационную систему, аттестованную по более высокому классу 3) Уничтожение по запросу субъекта 4) Получение согласия в письменной форме	ПК-10

2. Описание шкалы оценивания

Оценка успеваемости студентов по дисциплине осуществляется в ходе текущего контроля и промежуточной аттестации. Для проверки уровня сформированности компетенций используется совокупность оценочных средств, позволяющих оценить знания, умения и навыки, приобретённые студентами в процессе изучения дисциплины.

Основными формами текущего контроля являются:

– выполнение и защита лабораторных работ;

– устные опросы (собеседования) по темам занятий;

– проверка индивидуальных заданий;

– тестирование по отдельным разделам дисциплины.

Промежуточная аттестация проводится в форме экзамена и включает выполнение практического задания и/или ответы на теоретические вопросы.

3. Критерии оценивания компетенций заданий открытого типа

Оценка «отлично» выставляется студенту, если являются верными результаты демонстрации знаний об архитектуре ЭВМ (принципы фон Неймана, гарвардская архитектура, конвейеризация, кэш-память, иерархия памяти, механизмы защиты памяти — сегментация, страничная организация, кольца защиты), микропроцессорной технике (система команд, регистровая модель, режимы адресации, обработка прерываний и исключений, аппаратная поддержка безопасного выполнения кода — TrustZone, SGX и аналоги); а также знаний и умений в области соблюдения правовых норм, стандартов и требований информационной безопасности применительно к разработке низкоуровневого ПО и аппаратно-программных систем: способность участвовать в разработке нормативной и технической документации (технические задания, описания архитектуры, руководства по безопасности), учитывать законодательство в области ИТ (например, требования к обработке персональных данных, лицензирование ПО, экспортный контроль криптографических средств) при проектировании и отладке микропроцессорных устройств. Представленный отчёт (программный код на ассемблере/C, схемы, пояснения, документация по безопасности) не содержит ошибок, решены все задачи лабораторных работ и индивидуальных заданий. Компетенция **ПК-10** освоена на **высоком уровне**.

Оценка «хорошо» выставляется студенту, если являются верными результаты демонстрации указанных знаний и умений, но отчётный документ содержит незначительные ошибки, не влияющие на общий результат (например, неточности в оформлении технической документации, неполный учёт одного из стандартов безопасности), либо не представлены отдельные второстепенные задачи, не влияющие на общий результат. Компетенция **ПК-10** освоена на **среднем уровне**.

Оценка «удовлетворительно» выставляется студенту, если в основном верными являются результаты демонстрации знаний, но отчётный документ содержит ошибки, не позволяющие однозначно оценить качество разработки (например, неправильное применение механизмов защиты памяти, отсутствие анализа соответствия правовым нормам); представлены не все данные, задачи решены не в полном объёме. Компетенция **ПК-10** освоена на **минимальном уровне**.

Оценка «неудовлетворительно» выставляется студенту, если являются неверными результаты демонстрации знаний об архитектуре ЭВМ и микропроцессорной технике в контексте информационной безопасности и правовых норм, отчётный документ содержит много грубых ошибок (непонимание стандартов, отсутствие учёта законодательства, ошибки в защите памяти), не представлены ключевые данные (документация, схемы, обоснование безопасности), задачи не решены. Компетенция **ПК-10** не сформирована.

4. Критерии оценивания компетенций заданий закрытого типа

Оценка «отлично» выставляется студенту, если он правильно ответил на 88-100% от общего количества заданий. Компетенция ПК-10 освоена на высоком уровне.

Оценка «хорошо» выставляется студенту, если он правильно ответил на 72-87% от общего количества заданий. Компетенция ПК-10 освоена на среднем уровне.

Оценка «удовлетворительно» выставляется студенту, если он правильно ответил на 53-71% от общего количества заданий. Компетенция ПК-10 освоена на минимальном уровне.

Оценка «неудовлетворительно» выставляется студенту, выставляется студенту, если он правильно ответил на менее 53% от общего количества заданий. Компетенция ПК-10 не сформирована.