МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

Автоматизация технологических процессов и производств

УТВЕРЖДЕН
на заседании кафедры «23»
04.2026 г., протокол №10
Заведующий кафедрой
__________ Исаева М.Р.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Современные технологии защиты информации»

Направление подготовки

15.04.04 Автоматизация технологических процессов и производств

Направленность (профиль)

«Робототехнические системы автоматизированного управления»

Квалификация

магистр

Составитель (и) __________ И. М. Шабазов

Грозный – 2026

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Современные технологии защиты информации»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Теоретические основы информационной безопасности автоматизированных систем	ОПК-4, ПК-2	Практические работы Контрольная работа Тест Экзамен
2.	Защита автоматизированных систем управления и промышленных сетей	ОПК-4, ПК-2	Практические работы Контрольная работа Тест Экзамен
3.	Мониторинг, анализ и обеспечение устойчивости информационных систем	ОПК-4, ПК-2	Практические работы Контрольная работа Тест Экзамен
4.	Комплексная защита современных автоматизированных производственных систем	ОПК-4, ПК-2	Практические работы Контрольная работа Тест Экзамен

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Перечень оценочных средств
1.	Практическая работа	Средство для закрепления и практического освоения материала по определенному разделу	Комплект практических заданий
2.	Контрольная работа	Продукт самостоятельной работы студента, представляющий собой выполнения задания повышенной сложности по заданной теме	Комплект заданий
3.	Экзамен	Итоговая форма оценки знаний	Вопросы к экзамену

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1

«Анализ угроз и нормативное обеспечение информационной безопасности автоматизированных систем»

Перед выполнением получите вариант предприятия (АСУ ТП) у преподавателя.

Задание:

1. Провести анализ угроз для заданной АСУ ТП (не менее 5).
2. Определить перечень нормативных документов, регулирующих защиту информации на данном объекте.
3. Разработать организационные мероприятия по снижению выявленных рисков.
4. Составить таблицу соответствия «угроза → нормативный акт → организационная мера».

Отчет должен включать:

- таблицу угроз (источник, уязвимость, возможный ущерб);
- перечень нормативных документов с краткими выдержками;
- описание организационных мер (политики, регламенты, инструктажи);
- таблицу соответствия.

Практическая работа №2

Настройка механизмов защиты операционных систем и применение криптографических средств

Перед выполнением получите вариант конфигурации ОС (Windows/Linux) и тип криптосредства у преподавателя.

Задание:

1. Настроить политики безопасности ОС (парольная политика, аудит, контроль доступа).
2. Реализовать шифрование диска (или папки) с помощью штатных или сторонних средств.
3. Настроить электронную подпись для файлов конфигурации.
4. Описать последовательность действий и проверочные тесты.

Отчет должен включать:

- скриншоты настроек и результатов;
- таблицу примененных политик;
- описание алгоритма шифрования и ключевой информации;
- примеры проверки работоспособности.

Практическая работа №3

Реализация механизмов аутентификации, управления доступом и защиты промышленных сетей

Получите вариант топологии промышленной сети (с указанием устройств и протоколов) у преподавателя.

Задание:

1. Разработать схему разграничения доступа (роли, привилегии) для персонала АСУ ТП.
2. Настроить двухфакторную аутентификацию для удаленных инженеров.
3. Предложить меры по защите промышленной сети (VLAN, ACL, 802.1X).
4. Составить политику управления доступом и сетевыми правилами.

Отчет должен включать:

- матрицу доступа «роль – разрешенные действия»;
- описание и схему сегментации сети;
- настройки аутентификации (тип токенов, сервер RADIUS и т.п.);
- перечень правил межсетевого экранирования.

Практическая работа №4

Исследование защищенности SCADA-, PLC-систем и промышленного Интернета вещей

Получите вариант типа SCADA-системы, модели PLC и состава IIoT-устройств у преподавателя.

Задание:

1. Составить перечень потенциальных уязвимостей для каждого типа устройств.
2. Провести имитационное тестирование (в мысленном эксперименте) атак на протоколы (Modbus, S7, MQTT).
3. Предложить меры по усилению защиты (обновление, настройка, экранирование).
4. Разработать план регулярных проверок защищенности.

Отчет должен включать:

- таблицу уязвимостей по каждому устройству;
- описание сценариев атак и возможных последствий;
- рекомендуемые контрмеры;
- график аудитов и тестирований.

Практическая работа №5

Обеспечение безопасности баз данных, мониторинг событий и анализ инцидентов

Вариант: получите структуру БД (исторические данные, журналы, технологические параметры) и типовые события у преподавателя.

Задание:

1. Определить критичные данные и уровни их конфиденциальности.
2. Настроить политику резервирования и шифрования БД.
3. Спроектировать систему сбора и корреляции событий (SIEM) для промышленной сети.
4. Разработать регламент реагирования на инциденты (на примере одного типа атак).

Отчет должен включать:

- классификацию данных и требования к защите;

– схему резервного копирования и восстановления;
– структуру системы мониторинга (источники событий, правила корреляции);
– алгоритм действий при инциденте.

Практическая работа №6

Обеспечение отказоустойчивости, резервного копирования и оценка защищенности

Вариант: получите состав оборудования и требования по времени восстановления (RTO/RPO) у преподавателя.

Задание:

1. Разработать схему горячего/холодного резервирования для SCADA-серверов и контроллеров.
2. Составить регламент резервного копирования (периодичность, места хранения, проверка).
3. Провести качественную оценку защищенности (на основе контрольного перечня).
4. Предложить метрики для мониторинга готовности системы.

Отчет должен включать:

– схему резервирования (основное/резервное оборудование);
– таблицу с расписанием и способами резервного копирования;
– чек-лист оценка защищенности;
– показатели надежности и алгоритм аварийного переключения.

Практическая работа №7

«Проектирование комплексной системы защиты информации промышленного предприятия»

Перед началом выполнением практического задания получите свой вариант задания у преподавателя.

Задание:

1. Провести анализ угроз (не менее 5 актуальных для предприятия из вашего задания).
2. Разработать комплекс мер защиты (организационные + технические) с учетом бюджета и совместимости.
3. Предложить архитектурное решение (нарисовать схему сегментации сети, точек контроля, DMZ для удаленного доступа).
4. Составить поэтапный план внедрения на 1 год с указанием приоритетов и затрат по этапам.
5. Оценить остаточные риски (качественно: высокий/средний/низкий) после внедрения.

Отчет должен включать:

– таблицу угроз;
– таблицу предлагаемых мер;
– схему архитектуры;
– план-график с бюджетом;
– сравнительную оценку рисков «до/после».

Критерии оценки ответов на практических работы:

- не зачтено выставляется студенту, если *дан неполный ответ*, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

- зачтено выставляется студенту, если *дан полный, развернутый ответ* на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей.* Ответ изложен литературным языком в терминах науки. *Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.*

КОНТРОЛЬНАЯ РАБОТА СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

«Современные технологии защиты информации»

Контрольная работа выполняется в виде проекта по разработке комплекса мер обеспечения информационной безопасности автоматизированной системы управления технологическим процессом или робототехнического комплекса. Работа должна включать анализ объекта защиты, идентификацию угроз, выбор современных программно-аппаратных средств защиты информации, разработку организационных и технических мероприятий по обеспечению безопасности, а также обоснование предлагаемых решений.

Примерные темы контрольных работ:

1. Разработка системы защиты информации SCADA-системы промышленного предприятия.
2. Обеспечение информационной безопасности робототехнического комплекса.
3. Защита промышленной сети автоматизированного производственного участка.
4. Проектирование системы защиты информации автоматизированной линии производства.
5. Анализ угроз и разработка комплекса мер защиты для ПЛК и исполнительных устройств.
6. Обеспечение информационной безопасности промышленного Интернета вещей (IIoT).
7. Разработка политики информационной безопасности автоматизированного производственного предприятия.

Критерии оценки ответов по контрольным работам

- не зачтено выставляется студенту, если дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины. Подготовленная презентация не соответствует теме самостоятельной работы.

- зачтено выставляется студенту, если дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа. Подготовленная презентация соответствует теме самостоятельной работы.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д. МИЛЛИОНЩИКОВА

Институт энергетики

Кафедра Автоматизация технологических процессов и производств

Вопросы к экзамену по дисциплине «*Современные технологии защиты информации*»

Вопросы к экзамену:

1. Основные принципы обеспечения информационной безопасности автоматизированных систем управления. (ОПК-4)
2. Нормативно-правовая база и стандарты в области защиты информации автоматизированных систем. (ОПК-4)
3. Организационные и технические меры защиты информации на промышленном предприятии. (ОПК-4)
4. Классификация угроз информационной безопасности автоматизированных систем управления технологическими процессами. (ПК-2)
5. Особенности информационной безопасности робототехнических систем и комплексов. (ПК-2)
6. Механизмы защиты операционных систем, применяемых в автоматизированных системах управления. (ПК-2)
7. Современные методы криптографической защиты информации. (ПК-2)
8. Электронная подпись и инфраструктура открытых ключей. (ОПК-4, ПК-2)
9. Идентификация, аутентификация и управление доступом в автоматизированных системах. (ПК-2)
10. Принципы защиты промышленных сетей передачи данных. (ПК-2)
11. Межсетевые экраны, VPN и системы обнаружения вторжений в промышленных сетях. (ПК-2)
12. Архитектура и обеспечение безопасности SCADA-систем. (ПК-2)
13. Методы защиты программируемых логических контроллеров (PLC). (ПК-2)
14. Особенности обеспечения безопасности промышленного Интернета вещей (IIoT). (ПК-2)
15. Методы обеспечения безопасности баз данных автоматизированных систем управления. (ПК-2)
16. Мониторинг событий информационной безопасности и аудит автоматизированных систем. (ПК-2)
17. Методы обнаружения компьютерных атак и анализа инцидентов информационной безопасности. (ПК-2)
18. Анализ уязвимостей и оценка защищенности автоматизированных систем управления. (ПК-2)
19. Комплексная система защиты информации промышленного предприятия. (ОПК-4, ПК-2)
20. Применение современных технологий защиты информации при проектировании автоматизированных систем управления. (ПК-2)
21. Разработка организационно-распорядительной документации по

обеспечению информационной безопасности предприятия. (ОПК-4)

22. Перспективные направления развития технологий защиты информации в промышленной автоматизации и робототехнике. (ПК-2)

Критерии оценки ответов на экзамене

Оценка «отлично» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Современные технологии защиты информации»

ЭКЗАМЕНАЦИОННЫЕ МАТЕРИАЛЫ

2 СЕМЕСТР, ЭКЗАМЕН

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 1

1. Идентификация, аутентификация и управление доступом в автоматизированных системах. (ПК-2)
2. Методы защиты программируемых логических контроллеров (PLC).

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 2

1. Организационные и технические меры защиты информации на промышленном предприятии.
2. Основные принципы обеспечения информационной безопасности автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 3

1. Архитектура и обеспечение безопасности SCADA-систем.
2. Идентификация, аутентификация и управление доступом в автоматизированных системах. (ПК-2)

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 4

1. Разработка организационно-распорядительной документации по обеспечению информационной безопасности предприятия.
2. Особенности обеспечения безопасности промышленного Интернета вещей (IIoT).

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 5

1. Методы обеспечения безопасности баз данных автоматизированных систем управления.
2. Основные принципы обеспечения информационной безопасности автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 6

1. Анализ уязвимостей и оценка защищенности автоматизированных систем управления. Комплексная система защиты информации промышленного предприятия.
2. Особенности обеспечения безопасности промышленного Интернета вещей (IIoT).

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 7

1. Межсетевые экраны, VPN и системы обнаружения вторжений в промышленных сетях.
2. Основные принципы обеспечения информационной безопасности автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 8

1. Нормативно-правовая база и стандарты в области защиты информации автоматизированных систем.
2. Особенности обеспечения безопасности промышленного Интернета вещей (IIoT).

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 9

1. Архитектура и обеспечение безопасности SCADA-систем.
2. Перспективные направления развития технологий защиты информации в промышленной автоматизации и робототехнике.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 10

1. Организационные и технические меры защиты информации на промышленном предприятии.
2. Методы обеспечения безопасности баз данных автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 11

1. Современные методы криптографической защиты информации.
2. Анализ уязвимостей и оценка защищенности автоматизированных систем управления. Комплексная система защиты информации промышленного предприятия.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 12

1. Организационные и технические меры защиты информации на промышленном предприятии.
2. Применение современных технологий защиты информации при проектировании автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 13

1. Особенности обеспечения безопасности промышленного Интернета вещей (IIoT).
2. Применение современных технологий защиты информации при проектировании автоматизированных систем управления.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 14

1. Анализ уязвимостей и оценка защищенности автоматизированных систем управления. Комплексная система защиты информации промышленного предприятия.
2. Классификация угроз информационной безопасности автоматизированных систем управления технологическими процессами.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 15

1. Основные принципы обеспечения информационной безопасности автоматизированных систем управления.
2. Организационные и технические меры защиты информации на промышленном предприятии.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 16

1. Основные принципы обеспечения информационной безопасности автоматизированных систем управления.
2. Принципы защиты промышленных сетей передачи данных.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 17

1. Межсетевые экраны, VPN и системы обнаружения вторжений в промышленных сетях.
2. Разработка организационно-распорядительной документации по обеспечению информационной безопасности предприятия.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 18

1. Мониторинг событий информационной безопасности и аудит автоматизированных систем.
2. Принципы защиты промышленных сетей передачи данных.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 19

1. Мониторинг событий информационной безопасности и аудит автоматизированных систем.
2. Принципы защиты промышленных сетей передачи данных.

Подпись преподавателя_____
Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт энергетики
Группа "" Семестр "2"
Дисциплина "Современные технологии защиты информации"
Билет № 20

1. Архитектура и обеспечение безопасности SCADA-систем.
2. Межсетевые экраны, VPN и системы обнаружения вторжений в промышленных сетях.

Подпись преподавателя_____
Подпись заведующего кафедрой_____