МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ
Проректор по УР О.И. Варфоломеева

Подписано в СДОУ ELMA
Варфоломеева О. И.
06.02.2026 14:54

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение информационной безопасности а автоматизированных системах»

Регистрационный номер: 209. Дата регистрации: 06.02.2026.

Ижевск 2024

Глазовский инженерно-экономический институт

Составители программы:
Пронина И.В., канд. экон. наук, доцент (разделы 1, 4)
Горбушин А.Г., канд.пед.наук, доцент (разделы 2,3)

Образовательная программа рассмотрена и утверждена на заседании кафедры

Протокол от 22.12.2025 г. № 11

Образовательная программа разработана на основании Профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н; ФГОС 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021)

Заведующий кафедрой Горбушин Алексей Геннадьевич

Подписано в СДОУ ELMA
Горбушин А. Г.
04.02.2026 14:22

СОГЛАСОВАНО

ФИО согласующего	**Решение**	**Дата**
Верняева Регина Александровна	Согласовано	06.02.2026 9:21:01
Тарасова Мария Андреевна	Согласовано	06.02.2026 10:35:23

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Глазовский инженерно-экономический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Ижевский государственный технический университет имени М.Т. Калашникова»
(ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

УТВЕРЖДАЮ

Проректор по учебной работе

_____ О.И. Варфоломеева

«___»_____2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Обеспечение информационной безопасности в автоматизированных системах»

Глазов 2026

Ижевск 2024

Глазовский инженерно-экономический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Ижевский государственный технический университет имени М.Т. Калашникова»

Составители программы:
Пронина И.В., канд. экон. наук, доцент (разделы 1, 4)
Горбушин А.Г., канд.пед.наук, доцент (разделы 2,3)

Образовательная программа рассмотрена и утверждена на заседании кафедры «Машиностроение и информационные технологии»

Протокол от 22.12.2025 №11

Образовательная программа разработана на основании:
Профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н;
ФГОС 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021)

Заведующий кафедрой _____ А.Г. Горбушин

СОГЛАСОВАНО

Директор ИОТ _____ М.А. Тарасова

Начальник ОАиМР _____ М.С. Дмитриева

Разработчик программы _____ И.В. Пронина

Глазовский инженерно-экономический институт (филиал)
федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

УЧЕБНЫЙ ПЛАН
программы повышения квалификации
«Обеспечение информационной безопасности в автоматизированных системах»

Категория слушателей: – лица, имеющие высшее образование
Срок обучения: – 40 часов
Форма обучения: – очно-заочная

№ п/п	Наименование дисциплин (модулей, курсов), разделов, тем	Общая трудо-емкость, часов	Всего контактных часов		Контактные часы			СРС, часов	Форма контроля
			синхрон.	асинхрон.	лекции	лабораторные работы	практические и семинарские занятия		
1.	Основы информационной безопасности и нормативное регулирование для автоматизированных систем	8	2		2			6	Практическое задание
2.	Угрозы информационной безопасности в автоматизированных системах	8	2		2			6	Практическое задание
3.	Методы и средства защиты информации в автоматизированных системах	12	6		4		2	6	Практическое задание
4.	Практические аспекты обеспечения информационной безопасности типовой автоматизированной системы	11	5		2		3	6	Практическое задание
5.	Итоговая аттестация	1	1				1		зачет

Ижевск 2024

	Итого	**40**	**16**		**10**		**6**	**24**	

Глазовский инженерно-экономический институт (филиал)
федерального государственного бюджетного образовательного учреждения высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
программы повышения квалификации
«Обеспечение информационной безопасности в автоматизированных системах»

№ п/п	Наименование дисциплин (модулей, курсов), разделов, тем	Общая трудо-емкость, часов	Всего контактных часов		Контактные часы			СРС, часов	Форма контроля
			синхрон.	асинхрон.	лекции	лабораторные работы	практические и семинарские занятия		
1	**Основы информационной безопасности и нормативное регулирование для автоматизированных систем**	**8**	**2**		**2**			**6**	
1.1	Понятие и ключевые компоненты автоматизированных систем	4	1		0,5		0,5	3	Практическое задание
1.2	Специфика информационной безопасности в автоматизированных системах	4	1		0,5		0,5	3	Практическое задание
2	**Угрозы информационной безопасности в автоматизированных системах**	**8**	**2**		**2**			**6**	
2.1	Классификация угроз	4	1		0,5		0,5	3	Практическое задание
2.2	Векторы угроз (операционные системы, сети, прикладное ПО и СУБД)	4	1		0,5		0,5	3	Практическое задание
3	**Методы и средства защиты информации в автоматизированных системах**	**12**	**6**		**4**		**2**	**6**	
3.1	Организационные меры защиты информации	4	2		1		1	2	Практическое задание

3.2	Защита на уровне ОС и ПО	4	2		1		1	2	Практическое задание
3.3	Сетевые защиты	4	2		1		1	2	Практическое задание
4	**Практические аспекты обеспечения информационной безопасности (ИБ) типовой автоматизированной системы (АС)**	**11**	**5**		**2**		**3**	**6**	
4.1	Особенности защиты различных видов АС	5	2		1		1	3	Практическое задание
4.2	Жизненный цикл инцидента ИБ	6	3		1		2	3	Практическое задание
	Итоговая аттестация	1	1				1		зачет
	Итого	**40**	**16**		**10**		**6**	**24**	

Календарный учебный график
программы повышения квалификации
«Обеспечение информационной безопасности в автоматизированных системах»

Неделя	Лекции	Лабораторные работы	Практические и семинарские занятия	Самостоятельная работа	Промежуточная аттестация	Итоговая аттестация
1 неделя обучения	Тема 1.1 (0,5 часа) Тема 1.2 (0,5 часа) Тема 2.1 (0,5 часа) Тема 2.2 (0,5 часа) Тема 3.1 (1 час) Тема 3.2 (1 час) Тема 3.3 (1 час)		Тема 1.1 (0,5 часа) Тема 1.2 (0,5 часа) Тема 2.1 (0,5 часа) Тема 2.2 (0,5 часа) Тема 3.1 (1 час) Тема 3.2 (1 час) Тема 3.3 (1 час)	Тема 1.1 (3 часа) Тема 1.2 (3 часа) Тема 2.1 (3 часа) Тема 2.2 (3 часа) Тема 3.1 (2 часа) Тема 3.2 (2 часа) Тема 3.3 (2 часа)		
2 неделя обучения	Тема 4.1 (1 час) Тема 4.2 (1 час)		Тема 4.1 (1 час) Тема 4.2 (2часа)	Тема 4.1 (3 часа) Тема 4.2 (3часа)		зачет

«Обеспечение информационной безопасности в автоматизированных системах»

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Описание образовательной программы

Программа повышения квалификации «Обеспечение информационной безопасности в автоматизированных системах» направлена на обеспечение безопасности информации в автоматизированных системах.

Программа предназначена для специалистов по IT, администраторов, инженеров, руководителей проектов, ответственных за эксплуатацию и безопасность автоматизированных систем.

Программа разработана в соответствии с:

Профессиональным стандартом 06.033 Специалист по защите информации в автоматизированных системах, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н;

ФГОС 09.03.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 929 (ред. от 08.02.2021)

1.2 Цель образовательной программы

Цель реализации программы: сформировать у слушателей системные знания и практические навыки по обеспечению информационной безопасности (ИБ) автоматизированных систем различного уровня сложности, включая понимание угроз, методов защиты, требований нормативных документов и способов их практической реализации.

Компетенции (трудовые функции) в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах»:

B/09.6 Анализ уязвимостей внедряемой системы защиты информации.

1.3 Планируемые результаты обучения

Программа направлена на достижение слушателем следующих результатов обучения:

Знать:

З1 – способы защиты информации от несанкционированного доступа и утечки по техническим каналам;

З2 – нормативные правовые акты в области защиты информации;

З3 – организационные меры по защите информации.

Уметь:

У1 – классифицировать и оценивать угрозы безопасности информации автоматизированной системы;

У2 – разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы

У3 – проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств

У4 – устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.

1.4 Категория слушателей: слушатели, имеющие высшее образование.

1.5 Трудоемкость обучения: 40 академических часов.

1.6 Форма обучения: очная.

1.7 Применение ЭО и ДОТ: нет.

2 РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН

РАБОЧАЯ ПРОГРАММА КУРСА «Обеспечение информационной безопасности в автоматизированных системах»

Тема 1. Введение. Основы ИБ и нормативное регулирование для АС. (2 часа)

Вопросы, раскрывающие содержание темы:

1.1 Понятие автоматизированной системы. Ключевые компоненты АС: АРМ, серверы, сети, данные, приложения, персонал.

1.2 Специфика ИБ в АС: конфиденциальность, целостность, доступность. Обзор 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности КИИ». Роль ФСТЭК и ФСБ. Базовые понятия: модель нарушителя, угроза, уязвимость, риски ИБ.

Тема 2. Угрозы информационной безопасности в автоматизированных системах. (2 часа)

Вопросы, раскрывающие содержание темы:

2.1 Классификация угроз: внутренние/внешние, преднамеренные/непреднамеренные.

2.2 Векторы угроз: Угрозы на уровне операционных систем и рабочих станций. Угрозы на сетевом уровне (сетевая разведка, атаки типа DoS, MITM). Угрозы на уровне прикладного ПО и СУБД (инъекции, несанкционированный доступ к данным).

Тема 3. Методы и средства защиты информации в АС. (4 часа)

Вопросы, раскрывающие содержание темы:

3.1 Организационные меры: политики безопасности, регламенты, обучение пользователей. Идентификация, аутентификация и управление доступом (ИАА). Ролевая модель доступа.

3.2 Защита на уровне ОС и ПО: обновление, настройка политик, антивирусная защита.

3.3 Сетевые средства защиты: МЭ (файрволы), VPN, системы обнаружения вторжений (IDS/IPS). Криптографические средства: шифрование данных на дисках и в каналах связи, ЭП. Резервное копирование и восстановление как основа обеспечения доступности.

Тема 4. Практические аспекты обеспечения ИБ типовой АС. (2 часа)

Вопросы, раскрывающие содержание темы:

4.1 Особенности защиты АС, обрабатывающих персональные данные (ПДн). Особенности защиты АС, входящих в состав КИИ (критической информационной инфраструктуры). Подход к защите АС как к комплексной задаче («защищенный периметр» vs «глубокоэшелонированная оборона»).

4.2 Жизненный цикл инцидента ИБ: выявление, анализ, реагирование, устранение последствий.

Перечень практических занятий

Номер темы	Наименование практической работы
3	Настройка базовых средств защиты операционной системы. (2 часа). Работа с учетными записями и группами. Настройка политик паролей и блокировки учетных записей. Анализ и настройка прав доступа к файлам и папкам (NTFS/права Linux). Работа с журналами событий безопасности (Event Viewer / журналы аудита).
4	Анализ защищенности и реагирование на инциденты в АС. (3 часа) Проверка уязвимостей ПО, обновление систем. Моделирование инцидента (напр., фишинговая атака, подбор пароля). Алгоритм действий при обнаружении инцидента: изоляция узла, сбор артефактов, смена учетных данных, анализ. Разбор кейса по построению простой схемы защиты для типовой АС (сервер БД + рабочие места).

Самостоятельная работа

Номер темы	Содержание самостоятельной работы

1	1.1 Аналитический обзор нормативной базы (3 часа). Используя официальные сайты ФСТЭК России и Роскомнадзора, найдите и изучите следующие документы: - Приказ ФСТЭК России № 21 «Об утверждении Состава и содержатия организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». - Приказ ФСТЭК России № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах». Задача: Составьте сравнительную таблицу в свободной форме. В одной колонке укажите, для защиты какой категории объектов (ПДн или АСУ ТП КВО) предназначен каждый документ. В другой колонке выпишите по 2-3 ключевых технических требования из каждого (например, «регистрация событий безопасности», «управление доступом», «резервное копирование»). Сделайте вывод о различиях в акцентах регуляторов 1.2 Определение границ АС (3 часа) Кейс: Рассмотрите инфраструктуру вашей организации. Какие АС в ней используются? Задача: Определите, можно ли считать это единой АС? Если нет, предложите варианты разбиения на отдельные АС. Для каждой выделенной АС назовите главный информационный актив и сформулируйте для него основную цель ИБ (конфиденциальность/целостность/доступность)

2	Угрозы информационной безопасности в автоматизированных системах. Задание 2.1: Построение карты угроз для типового компонента (3 часа) 1. Выберите один компонент АС: Веб-сервер (Apache/Nginx). 2. Используя открытые источники (базы уязвимостей CVE, материалы PTES), составьте карту угроз в виде схемы или списка. Уровень 1: Угрозы операционной системе, на которой работает сервер (например, эксплуатация уязвимостей RCE). Уровень 2: Угрозы самому веб-серверу (настройки по умолчанию, DDoS). Уровень 3: Угрозы веб-приложению, которое он обслуживает (SQL-инъекции, XSS). Для каждой угрозы кратко укажите возможные последствия (нарушение C, I или A). Задание 2.2: Анализ реального инцидента (3 часа) Найдите в открытых СМИ (Хабр, SecurityLab, RB.RU) описание одного реального инцидента ИБ, связанного со взломом корпоративной системы. Задача: По шаблону ответьте на вопросы: 1. Вектор атаки: Как злоумышленник проник в систему? (Фишинг, уязвимость, иное). 2. Цель: Что было целью? (Данные, деньги, нарушение работы). 3. Компонент АС: Какой компонент АС был атакован? (Пользователь, ПО, сеть). 4. Причина успеха атаки: В чем была ключевая ошибка/слабость защиты?

3	Методы и средства защиты информации в АС Задание 3.1: Сравнительный анализ средств защиты (3 час) 1. Выберите одну категорию средств защиты: Вариант А: Сетевые МЭ/Фаерволы нового поколения (NGFW). Вариант Б: Системы предотвращения утечек данных (DLP). 2. Проведите исследование, изучив сайты вендоров (Cisco, Palo Alto, Fortinet для NGFW; InfoWatch, Zecurion, Symantec для DLP) и независимые обзоры. 3. Задача: Напишите краткий отчет (не более 1 страницы), который должен содержать: Основные функции данного класса средств. На каких уровнях модели OSI/какие угрозы он парирует. Примеры 2-3 конкретных продуктов и их ключевые особенности. Ваш вывод о том, для какого типа АС (масштаб, отрасль) данный класс средств является критически важным. Задание 3.2: Разработка инструкции пользователя (3 часа) Контекст: В компании внедряется новая АС «CRM-Система». Необходимо подготовить раздел «Меры информационной безопасности» для инструкции пользователя. Задача: Составьте этот раздел. Он должен включать понятные и конкретные правила по следующим пунктам: 1. Парольная политика: Требования к созданию и хранению пароля. 2. Работа с данными: Что можно и нельзя делать с конфиденциальными данными из системы (печать, копирование, пересылка). 3. Действия при подозрительных событиях: (Пришло странное письмо с ссылкой «от администратора», забыл разлогиниться на чужом ПК). 4. Ответственность. Формат — нумерованный список или памятка.

4	Практические аспекты обеспечения ИБ типовой АС Задание 4.1: Проектирование архитектуры безопасности для кейса (3 часа) Кейс для проектирования: Разработайте архитектуру безопасности для АС «Умный дом» жилого комплекса. АС включает: центральный сервер управления, IP-камеры, датчики (протечки, открытия дверей), управление шлагбаумами, личные кабинеты жильцов в мобильном приложении. Задача: Нарисуйте схематичную диаграмму (блок-схему) этой АС и нанесите на нее средства защиты, используя условные обозначения. В пояснительной записке к схеме опишите: Как обеспечена сегментация сети (отдельные VLAN для камер, для датчиков, для сервера). Как организован контроль доступа к серверу и мобильному приложению. Как защищена целостность и конфиденциальность данных (шифрование, ЭП). Как гарантируется доступность системы при сетевых атаках. Задание 4.2: Расчет рисков и разработка плана мероприятий (3 часа) 1. Используйте результаты Задания 2.1 (Карта угроз для веб-сервера). 2. Задача: Проведите упрощенную качественную оценку рисков и составьте План мероприятий по их снижению в виде таблицы. Угроза (из Задания 2.1) Вероятность (Низкая/Средняя/Высокая) Влияние (Низкое/Среднее/Высокое) Мера по снижению риска Тип меры (Техн./Орг.) Пример: DDoS-атака Средняя Высокое Заключение договора с провайдером на услугу очистки трафика (Anti-DDoS) Техническая SQL-инъекция Высокая Высокое 1. Регулярный pentest веб-приложения. 2. Внедрение WAF. Техническая Для 3-4 наиболее опасных угроз предложите конкретные, реализуемые меры защиты.

3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы включает текущую и итоговую аттестацию обучающихся.

3.1 Формы текущей и итоговой аттестации

Текущая аттестация проводится по результатам выполнения практических заданий.

Итоговая аттестация проводится в форме зачета.

Итоговая аттестация осуществляется преподавателем программы на основе двухбалльной («зачтено», «не зачтено») системе оценок.

3.2 Оценочные материалы

Примерный тест для итоговой аттестации по программе «Обеспечение информационной безопасности в автоматизированных системах»

Инструкция: Выберите один или несколько правильных ответов.

1. Автоматизированная система (АС) – это:

а) Только компьютерное оборудование.

б) Комплекс аппаратных и программных средств, предназначенный для автоматизации бизнес-процессов.

в) Любая система, в которой используется компьютер.

г) Совокупность персонала и информационных технологий, выполняющая определенную функцию.

2. Какие из перечисленных нормативных актов являются базовыми для регулирования ИБ в РФ? (Выберите два основных)

а) Трудовой кодекс РФ.

б) 152-ФЗ «О персональных данных».

в) ГОСТ Р ИСО 9001.

г) 187-ФЗ «О безопасности критической информационной инфраструктуры».

3. Какая из трех ключевых целей информационной безопасности (триада CIA) наиболее критична для системы диспетчеризации энергосети?

а) Конфиденциальность.

б) Целостность.

в) Доступность.

г) Все цели равнозначны.

4. Какой метод защиты в первую очередь предназначен для противодействия угрозам социальной инженерии?

а) Установка межсетевого экрана.

б) Шифрование жесткого диска.

в) Регулярное обучение и информирование пользователей.

г) Настройка сложной политики паролей.

5. Что из перечисленного является ОРГАНИЗАЦИОННОЙ мерой защиты информации в АС?

а) Настройка системы антивирусного мониторинга.

б) Разработка и введение в действие «Инструкции пользователя АС по соблюдению требований ИБ».

в) Установка системы обнаружения вторжений (IDS).

г) Внедрение системы шифрования VPN-каналов.

6. Какой класс средств защиты информации обеспечивает проверку личности пользователя?

а) Средства резервного копирования.

б) Средства аутентификации.

в) Средства анализа сетевого трафика.

г) Средства антивирусной защиты.

7. Основная цель настройки межсетевого экрана (брандмауэра) на границе сети АС:

а) Ускорить работу интернет-соединения.

б) Фильтровать входящий и исходящий сетевой трафик на основе правил.

в) Шифровать весь трафик внутри сети.

г) Автоматически исправлять ошибки в программном коде.

8. Какая мера является обязательной для защиты АС, обрабатывающей персональные данные в соответствии с 152-ФЗ?

а) Получение лицензии ФСБ.

б) Назначение ответственного за организацию обработки ПДн и реализация мер, предусмотренных законодательством.

в) Ежедневное шифрование всех архивов.

г) Обязательная сертификация всех используемых программ.

9. Что из перечисленного НЕ является типовой угрозой на уровне операционной системы АРМ?

а) Эксплуатация уязвимостей в необновленном ПО.

б) SQL-инъекция через веб-форму.

в) Запуск вредоносного кода, полученного по email.

г) Несанкционированный доступ к файлам из-за слабых прав доступа.

10. Какая практика является основой для обеспечения доступности данных в АС при сбое оборудования?

а) Использование аппаратного RAID-массива.

б) Регулярное резервное копирование с проверкой восстановления.

в) Хранение всех данных в облачном сервисе.

г) Установка двух мониторов на каждое рабочее место.

11. Какая из перечисленных атак напрямую направлена на нарушение ЦЕЛОСТНОСТИ информации в АС?

а) Перехват пароля по сети.

б) Внесение несанкционированных изменений в базу данных.

в) DDoS-атака на веб-сервер.

г) Копирование конфиденциального документа.

12. Принцип «минимально необходимых привилегий» в управлении доступом означает, что:

а) Все пользователи должны иметь пароль длиной не менее 12 символов.

б) Пользователю должны быть выданы права доступа, строго необходимые для выполнения его рабочих задач.

в) Администратор должен иметь доступ ко всем системам в любое время.

г) Доступ к системе должен предоставляться только в рабочее время.

13. Что является первым рекомендуемым действием при обнаружении инцидента ИБ (например, заражения вирусом) на рабочей станции в составе АС?

а) Немедленно перезагрузить компьютер.

б) Отключить рабочую станцию от сети (физически или логически) для локализации угрозы.

в) Позвонить в службу технической поддержки ПО.

г) Продолжить работу, чтобы сохранить важные данные.

14. Для защиты от угрозы «Человек посередине» (MitM) на сетевом уровне в первую очередь применяют:

а) Антивирусное ПО.

б) Технологии шифрования канала связи (например, TLS/SSL, VPN).

в) Сложные пароли.

г) Системы резервного копирования.

15. Аудит событий безопасности в АС проводится в основном для:

а) Увеличения производительности серверов.

б) Последующего анализа действий пользователей и системных событий для выявления инцидентов и нарушений.

в) Автоматического исправления всех найденных уязвимостей.

г) Отключения неиспользуемых учетных записей.

Критерии оценки итоговой аттестационной работы:

Оценка	***Критерии оценки***
«зачтено»	Обучающимся дано 60% правильных ответов
«не зачтено»	Обучающимся дано менее 60% правильных ответов

Примерные практические задания для текущей аттестации:

Тема 1: Введение. Основы ИБ и нормативное регулирование для АС.

Задание 1.1. «Определение границ и активов АС»

Описание: Вам предоставлено описание компании «Омега» (малое торговое предприятие). В ее ИТ-инфраструктуру входят: 1) Сервер с 1С:Бухгалтерия (база клиентов и финансов), 2) 5 компьютеров сотрудников, 3) Маршрутизатор с выходом в интернет, 4) Принтер в общей сети.

Задача: На основании описания выделите автоматизированную систему (АС) и ее ключевые компоненты. Определите, какой из активов АС является наиболее критичным с точки зрения нарушения конфиденциальности, целостности и доступности. Ответ обоснуйте.

Критерий оценивания: Корректное выделение АС (ядро — Сервер 1С и рабочие места для доступа к нему) и ее компонентов. Аргументированное определение критичного актива (сервер 1С) и анализ рисков для него по триаде CIA.

Задание 1.2. «Нормативная привязка»

· писание: Та же компания «Омега» начала обработку персональных данных сотрудников и клиентов в системе 1С.

Задача: Перечислите основные нормативные документы (законы, приказы регуляторов), требования которых теперь должна учитывать «Омега». Кратко (1-2 предложения) сформулируйте одно практическое следствие из каждого документа для администратора АС.

Критерий оценивания: Знание 152-ФЗ, приказов ФСТЭК №21, 17 (или актуальных). Качественное предложение мер (напр., по 152-ФЗ: «Требуется назначить ответственного и составить модель угроз»).

Тема 2: Угрозы информационной безопасности в автоматизированных системах.

Задание 2.1. «Классификация инцидента»

Описание: Вам представлены три инцидента в АС:

1. Сотрудник по ошибке удалил важный каталог с файлами с файлового сервера.
2. На web-сервере АС обнаружена уязвимость, позволяющая через форму ввода получить доступ к базе данных.
3. Злоумышленник отправил сотруднику письмо с вредоносным вложением, маскируя его под счет.

Задача: Для каждого инцидента определите:

Ключевой нарушаемый аспект ИБ (конфиденциальность/целостность/доступность).

Класс угрозы (внутренняя/внешняя, преднамеренная/непреднамеренная).

Компонент АС, на который направлена угроза (данные, ПО, пользователь).

Критерий оценивания: Точность классификации по всем трем параметрам для каждого инцидента.

Тема 3: Методы и средства защиты информации в АС.

Задание 3.1. «Разработка политики паролей»

Описание: В организации действует простая политика паролей: длина 6 символов, без требований к сложности. Участились случаи подбора паролей.

Задача: Используя оснастку «Локальная политика безопасности» (Windows) или файлы конфигурации PAM (Linux), настройте на виртуальной машине более строгую политику. Параметры: минимальная длина пароля — 10 символов, требование к сложности (заглавные, строчные, цифры), блокировка учетной записи после 5 неудачных попыток на 15 минут. Предоставьте скриншоты настроек.

Критерий оценивания: Технически правильная реализация всех трех требований в среде.

Тема 4: Практические аспекты обеспечения ИБ типовой АС.

Задание 4.1. «Проектирование схемы защиты для АС» (Комплексный кейс)

Описание: Компания «Дельта» разрабатывает АС «Складской учет». АС состоит из: сервера приложений (веб-интерфейс), сервера БД, 10 рабочих мест кладовщиков в отдельной сети склада. Обрабатываются коммерческие тайны (номенклатура, остатки).

Задача: Разработайте краткую схему (архитектуру) защиты АС. Включите в схему не менее 5 технических и организационных мер, распределив их по компонентам (рабочие места, внутренняя сеть, сервера). Обоснуйте выбор каждой меры. (Пример: 1. На рабочих местах: запрет USB-портов через групповые политики для предотвращения утечки. 2. В сети: сегментирование — VLAN для сети склада для ограничения распространения угроз... и т.д.).

Критерий оценивания: Комплексность подхода, увязка мер с конкретными угрозами, реалистичность предложений.

Задание 4.2 «Разработка регламента резервного копирования»

Описание: Для АС, описанной в задании 4.1, критичными являются данные в БД (остатки товаров) и конфигурационные файлы веб-приложения.

Задача: Составьте краткий регламент (инструкцию) резервного копирования. Включите пункты:

Что подлежит копированию (объекты).

Где хранятся копии (не менее 2 локаций).

Как часто выполняется (периодичность).

Кто отвечает.

Как проверяется возможность восстановления (периодичность теста).

Критерий оценивания: Полнота охвата ключевых параметров политики резервирования, практическая применимость, учет требования доступности.

Общие критерии оценки практических заданий:

«Отлично»: Задание выполнено полностью, корректно, предложены нестандартные/оптимальные решения. Отчет представлен четко.

«Хорошо»: Задание выполнено с незначительными недочетами. Основная цель достигнута.

«Удовлетворительно»: Задание выполнено частично, с ошибками, но общий подход понятен.

«Неудовлетворительно»: Задание не выполнено или выполнено с критическими ошибками, демонстрирующими непонимание темы.

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

4.1. Требования к квалификации педагогических кадров

Реализацию программы повышения квалификации осуществляют педагогические работники кафедры «Машиностроение и информационные технологии», имеющие профильное высшее образование и (или) ученую степень, ученое звание, профессиональную переподготовку по профилю программы и (или) привлеченные ведущие специалисты предприятий и организаций, осуществляющие профессиональную деятельность в предметной области программы.

4.2. Материально-технические условия реализации программы

Наименование специализированных	Вид занятий	Наименование оборудования, программного обеспечения

аудиторий, кабинетов, лабораторий		
1	2	3
Аудитория № 209	Лекционные и практические занятия	Учебная мебель, проектор - 1 шт., персональный компьютер – 11 шт. с доступом к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации

4.3. Учебно-методическое обеспечение программы

Основная литература:

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html

Перечень ресурсов информационно-коммуникационной сети Интернет

1. Электронно-библиотечная система **IPRbooks** http://istu.ru/material/elektronno-bibliotechnaya-sistema-iprbooks
2. Электронный каталог научной библиотеки ИжГТУ имени М.Т. Калашникова **Web ИРБИС** http://94.181.117.43/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=IBIS&P21DBN=IBIS
3. **Национальная электронная библиотека -** http://нэб.рф.
4. Мировая цифровая библиотека - http://www.wdl.org/ru/
5. Международный индекс научного цитирования **Web of Science –** http://webofscience.com.
6. **Научная электронная библиотека eLIBRARY.RU –** https://elibrary.ru/defaultx.asp

5. РУКОВОДСТВО И СОСТАВИТЕЛИ ПРОГРАММЫ

Руководитель программы:

Горбушин Алексей Геннадьевич, к.п.н, доцент, доцент кафедры «Машиностроение и информационные технологии», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».

Составители программы:

Пронина Ирина Викторовна, к.э.н., доцент, доцент кафедры «Экономика и менеджмент», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».

Горбушин Алексей Геннадьевич, к.п.н, доцент, доцент кафедры «Машиностроение и информационные технологии», ГИЭИ (филиал) ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова».