

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: бакалавриат

Форма обучения: очная

Программа
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Блок	Блок 3 «Государственная итоговая аттестация»
Трудоемкость в зачетных единицах	8 семестр – 6
Часов (всего) по учебному плану	216
включая: подготовку к сдаче и сдачу государственного экзамена подготовку к процедуре защиты и защиту выпускной квалификационной работы	учебным планом не предусмотрены 8 семестр – 216 часов

ПРОГРАММУ СОСТАВИЛ:

Доцент кафедры безопасности и
информационных технологий, к.т.н.,
доцент

(должность, ученая степень, ученое звание)



(подпись)

О.Р. Баронов

(расшифровка подписи)

Заведующий кафедрой безопасности
и информационных технологий

(название кафедры)



(подпись)

А.Ю. Невский

(расшифровка подписи)

Руководитель образовательной программы

Доцент кафедры безопасности и
информационных технологий, к.т.н.,
доцент

(должность, ученая степень, ученое звание)



(подпись)

О.Р. Баронов

(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Целью государственной итоговой аттестации является оценка подготовленности обучающегося к решению задач профессиональной деятельности.

Задачами государственной итоговой аттестации:

- оценка сформированности всех компетенций, установленных образовательной программой
- оценка освоения результатов обучения требованиям федерального государственного образовательного стандарта по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 17.11.2020 г. № 1427, зарегистрированным в Минюсте России 18.02.2021 г., регистрационный номер 62548. Профессиональный стандарт 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальных отношений Российской Федерации № 598н от 01.11.2016 г., рег.номер 842; Профессиональный стандарт 06.033 «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальных отношений Российской Федерации № 522н от 15.09.2016 г., рег.номер 843; Профессиональный стандарт 06.034 «Специалист по технической защите информации», утвержденный приказом Министерства труда и социальных отношений Российской Федерации № 599н от 01.11.2016 г., рег.номер 844.

2. ОБЩЕКУЛЬТУРНЫЕ (УНИВЕРСАЛЬНЫЕ), ОБЩЕПРОФЕССИОНАЛЬНЫЕ И ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ, УСТАНОВЛЕННЫЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММОЙ

2.1. Универсальные компетенции выпускников

Категория универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1 _{УК-1} . Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи ИД-2 _{УК-1} . Использует системный подход для решения поставленных задач
разработка и реализация проекта	УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИД-1 _{УК-2} . Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение ИД-2 _{УК-2} . Выбирает наиболее эффективный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения
командная работа и лидерство	УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	ИД-1 _{УК-3} . Определяет стратегию сотрудничества для достижения поставленной цели ИД-2 _{УК-3} . Взаимодействует с другими членами команды для достижения поставленной задачи

коммуникация	УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	ИД-1 _{УК-4} . Демонстрирует умение вести обмен деловой информацией в устной и письменной формах на государственном языке ИД-2 _{УК-4} . Демонстрирует умение вести обмен деловой информацией в устной и письменной формах не менее чем на одном иностранном языке
межкультурное взаимодействие	УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	ИД-1 _{УК-5} . Анализирует современное состояние общества на основе знания истории ИД-2 _{УК-5} . Интерпретирует проблемы современности с позиций этики и философских знаний ИД-3 _{УК-5} . Демонстрирует понимание общего и особенного в развитии цивилизаций, религиозно-культурных отличий и ценностей локальных цивилизаций
самоорганизация и само развитие (в том числе здоровьесбережение)	УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	ИД-1 _{УК-6} . Эффективно планирует собственное время ИД-2 _{УК-6} . Планирует траекторию своего развития и предпринимает шаги по её реализации
самоорганизация и само развитие (в том числе здоровьесбережение)	УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	ИД-1 _{УК-7} . Понимает влияние оздоровительных систем физического воспитания на укрепление здоровья, профилактику профессиональных заболеваний ИД-2 _{УК-7} . Выполняет индивидуально подобранные комплексы оздоровительной или адаптивной физической культуры
безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	ИД-1 _{УК-8} . Выявляет возможные угрозы для жизни и здоровья человека, и природной среды, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов ИД-2 _{УК-8} . Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций ИД-3 _{УК-8} . Демонстрирует знание приемов оказания первой помощи пострадавшему

		ИД-4 _{УК-8} . Демонстрирует понимание влияния объектов профессиональной деятельности на состояние природной среды и устойчивое развитие общества
экономическая культура, в том числе финансовая грамотность	УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	ИД-1 _{УК-9} . Демонстрирует знание основных экономических принципов функционирования общества
гражданская позиция	УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	ИД-1 _{УК-10} . Демонстрирует способность выявлять коррупционное поведение и содействовать его пресечению ИД-2 _{УК-10} . Анализирует причины и условия способствующие коррупционному поведению

2.2. Общепрофессиональные компетенции выпускников

Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-1 _{ОПК-1} . Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации ИД-2 _{ОПК-1} . Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства
	ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД-1 _{ОПК-2} . Применяет информационно-коммуникационные технологии, в том числе отечественного производства для решения задач профессиональной деятельности ИД-2 _{ОПК-2} . Применяет программно-аппаратные средства и средства системного назначения, инструментальные средства, в том числе отечественного производства для решения профессиональных задач ИД-3 _{ОПК-2} . Применяет программные средства прикладного назначения, в том числе отечественного

		производства для решения профессиональных задач
	ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ИД-1 _{ОПК-3} . Применяет соответствующие математические методы для решения профессиональных задач ИД-2 _{ОПК-3} . Применяет соответствующий математический аппарат для решения профессиональных задач
	ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ИД-1 _{ОПК-4} . Анализирует физические явления и процессы для решения профессиональных задач ИД-2 _{ОПК-4} . Применяет положения электротехники, электроники и схемотехники для решения профессиональных задач
безопасность автоматизированных систем	ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ИД-1 _{ОПК-4.1} . Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации ИД-2 _{ОПК-4.1} . Готовит документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе
безопасность автоматизированных систем	ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ИД-1 _{ОПК-4.2} . Устанавливает и настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации
безопасность автоматизированных систем	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ИД-1 _{ОПК-4.3} . Применяет типовые программные средства резервирования и восстановления информации в автоматизированных системах ИД-2 _{ОПК-4.3} . Применяет программные средства обеспечения безопасности данных

безопасность автоматизированных систем	ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ИД-1 _{ОПК-4.4.} Выполняет обнаружение и идентификацию инцидентов в процессе эксплуатации автоматизированной системы ИД-2 _{ОПК-4.4.} Оценивает защищенность автоматизированных систем с помощью типовых программных средств ИД-3 _{ОПК-4.4.} Выполняет инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах
	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-1 _{ОПК-5.} Использует основы правовых знаний в различных сферах деятельности ИД-2 _{ОПК-5.} Использует нормативные правовые акты в профессиональной деятельности
	ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1 _{ОПК-6.} Оформляет рабочую техническую документацию с учетом действующих нормативных и методических документов ИД-2 _{ОПК-6.} Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты ИД-3 _{ОПК-6.} Организует технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ИД-1 _{ОПК-7.} Применяет программные средства специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ИД-2 _{ОПК-7.} Применяет технологии и методы разработки и внедрения прикладного программного

		обеспечения для решения задач профессиональной деятельности
	ОПК-8. Способен осуществлять подбор, изучение и общение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ИД-1 _{ОПК-8} . Выполняет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
	ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1 _{ОПК-9} . Настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации
	ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД-1 _{ОПК-10} . Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты ИД-2 _{ОПК-10} . Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации
	ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ИД-1 _{ОПК-11} . Проводит эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов ИД-2 _{ОПК-11} . Принимает участие в проведении экспериментальных исследований системы защиты информации
	ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИД-1 _{ОПК-12} . Проводит анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвует в проведении технико-экономического обоснования соответствующих проектных решений
	ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования	ИД-1 _{ОПК-13} . Анализирует основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма

	гражданской позиции и развития патриотизма	
--	--	--

2.3. Профессиональные компетенции выпускников

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-1. Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ПК-1.1 _{ПК-1} . Администрирует системы защиты информации автоматизированных систем ПК-1.2 _{ПК-1} . Управляет защитой информации в автоматизированных системах ПК-1.3 _{ПК-1} . Выполняет мониторинг защищенности информации в автоматизированных системах ПК-1.4 _{ПК-1} . Выполняет аудит защищенности информации в автоматизированных системах
ПК-2. Готов к внедрению систем защиты информации автоматизированных систем	ПК-2.1 _{ПК-2} . Устанавливает и настраивает средства защиты информации в автоматизированных системах ПК-2.2 _{ПК-2} . Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах ПК-2.3 _{ПК-2} . Внедряет организационные меры по защите информации в автоматизированных системах
ПК-3. Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.1 _{ПК-3} . Администрирует подсистемы защиты информации в операционных системах ПК-3.2 _{ПК-3} . Администрирует программно-аппаратные средства защиты информации в компьютерных сетях ПК-3.3 _{ПК-3} . Администрирует средства защиты информации прикладного и системного программного обеспечения
ПК-4. Способен проводить контроль защищенности информации	ПК-4.1 _{ПК-4} . Способен проводить специальные исследования на побочные электромагнитные излучения и наводки технических средств обработки информации ПК-4.2 _{ПК-4} . Способен проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок ПК-4.3 _{ПК-4} . Способен проводить контроль защищенности акустической речевой информации от утечки по техническим каналам

3. ФОРМА, СРОКИ И ТРУДОЕМКОСТЬ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Общая трудоемкость государственной итоговой аттестации составляет 6 зачетных единиц, 216 часов.

Государственная итоговая аттестация является завершающей частью образовательной программы и проводится в 8 семестре после успешного прохождения промежуточной аттестации по всем дисциплинам (модулям) и практикам образовательной программы.

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы.

В государственную итоговую аттестацию входит подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы.

4. КРАТКОЕ СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИН, ВКЛЮЧЕННЫХ В ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН

Государственный экзамен учебным планом не предусмотрен.

5. ПРИМЕРНАЯ ТЕМАТИКА ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

6. Защита персональных данных финансово-кредитной организации
7. Защита персональных данных в коммерческой организации
8. Защита персональных данных в организации с участием государства (муниципальном образовании)
9. Защита персональных данных в медицинских учреждениях
10. Защита электронного документооборота на предприятии
11. Инвентаризация информационных активов организации
12. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере организации малого (среднего) бизнеса)
13. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере финансово-кредитного учреждения)
14. Защита коммерческой тайны в организации
15. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации)
16. Защита информации в концепции стандарта ISO 27001 (на примере некоммерческой организации)
17. Защита служебной тайны в организации
18. Защита интеллектуальной собственности в организации
19. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001
20. Аттестация системы информационной безопасности государственной информационной системы
21. Разработка модели угроз информационной безопасности в финансово-кредитном учреждении
22. Разработка модели нарушителя информационной безопасности в организации
23. Разработка модели нарушителя информационной безопасности в организации, относящейся к критической информационной инфраструктуре
24. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам
25. Имитационное моделирование сценариев рисков информационной безопасности
26. Анализ рисков информационной безопасности в информационной системе персональных данных
27. Мониторинг состояния объекта на основе оценки рисков
28. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей

29. Моделирование рисков информационной безопасности в информационных системах, построенных по технологии блокчейн
30. Инвентаризация и классификация информационных активов организации при оценке рисков
31. Оценка и анализ рисков с использованием программного обеспечения CORAS
32. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики
33. Разработка комплекта документации по результатам аттестации объекта информатизации (автоматизированной системы)
34. Разработка политики информационной безопасности организации
35. Разработка комплекса мероприятий по лицензированию деятельности предприятия по технической защите конфиденциальной информации
36. Разработка комплекса мероприятий по сертификации средства обработки конфиденциальной информации
37. Разработка комплекса мероприятий по сертификации средства защиты информации
38. Организация режима коммерческой тайны на предприятии
39. Разработка частных политик информационной безопасности для организации
40. Моделирование угроз персональным данным в организации
41. Обеспечение безопасности информации на объектах критической информационной инфраструктуры
42. Документальное обеспечение режима коммерческой тайны предприятия
43. Формирование требований к сотруднику службы информационной безопасности при внедрении профессиональных стандартов
44. Разработка и реализация программы повышения осведомленности сотрудников предприятия (организации) в области информационной безопасности
45. Организация проверки и оценки уровня подготовки персонала предприятия, участвующего в обработке конфиденциальной информации
46. Управление поведением персонала при организации безопасной работы в информационной системе организации
47. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию
48. Подготовка персонала организации, использующего в работе конфиденциальную информацию с использованием дистанционных образовательных технологий
49. Организация расследования инцидентов информационной безопасности на предприятии
50. Обеспечение режима конфиденциальности в организации при увольнении сотрудников
51. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики)
52. Разработка проекта технической защиты конфиденциальной информации на предприятии от ее утечки по (конкретный вид) каналу
53. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу
54. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов
55. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия
56. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия

57. Разработка программы специального обследования защищаемого помещения (кабинета, переговорной комнаты, конференц-зала и т.д.) предприятия (организации)
58. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии
59. Разработка технического проекта создания защищаемого помещения в организации
60. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи
61. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации
62. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ
63. Разработка проекта системы защиты конфиденциальной информации в организации
64. Разработка предложений по повышению защищенности вычислительной техники по каналу ПЭМИ пассивными методами
65. Разработка рекомендаций по защите конфиденциальной информации от утечки по акустическому каналу из защищаемого помещения пассивными методами
66. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга
67. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации
68. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места
69. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN
70. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах
71. Программная защита информационной системы организации на основе возможностей операционной системы
72. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows
73. Разработка и внедрение электронной подписи в документооборот организации
74. Анализ уязвимостей систем удаленного видеонаблюдения на предприятии
75. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN
76. Администрирование средств межсетевого экранирования в системе защиты информации организации
77. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации
78. Администрирование системы резервного копирования для защиты информационных активов организации
79. Внедрение в организации системы резервного копирования
80. Обеспечение безопасности сетевого взаимодействия с использованием технологии IPSec
81. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных
82. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных
83. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux

84. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux
85. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux
86. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux
87. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации
88. Защита локальной вычислительной сети организации с использованием IDS/IPS систем
89. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации
90. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа
91. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации
92. Разработка средств автоматизации для исследования программного обеспечения по требованиям безопасности информации
93. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации»)
94. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет
95. Применение систем контроля и управления процессами («вывода на печать» или «вывода на внешние носители информации» или «отправки файлов через интернет» или «отправки файлов по электронной почте») в (название организации)
96. Защита от несанкционированных проводных подключений к локальной сети (название организации)
97. Организация аудита информационной безопасности организации с использованием специального программного обеспечения
98. Применение технологии активного аудита информационной безопасности в организации
99. Разработка программы проведения аудита информационной безопасности в организации
100. Разработка программы проведения внутреннего аудита информационной безопасности организации
101. Внедрение системы менеджмента инцидентов информационной безопасности в коммерческом банке
102. Организация мониторинга действий персонала организации с целью выявления инцидентов информационной безопасности
103. Внедрение технологий предотвращения утечки информации (DLP-системы) в организации
104. Внедрение технологии управления информацией и событиями безопасности (SIEM-системы) в организации
105. Автоматизация процессов менеджмента информационной безопасности в организации
106. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении
107. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении
108. Организация центра управления информационной безопасностью в финансово-кредитном учреждении

109. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении
110. Расследование инцидентов информационной безопасности в организации
111. Проведение аудита информационной безопасности организации с использованием сканера безопасности
112. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности
113. Защита информации с использованием методов и технологий упрощенной криптографии в организации
114. Криптографические способы контроля целостности и их практическая реализация
115. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании
116. Моделирование уязвимостей протоколов защиты TLS
117. Моделирование уязвимостей протоколов защиты SSL
118. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos
119. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков
120. Обеспечение информационной безопасности Интернета вещей в цифровой экономике
121. Исследование механизмов целостности и доступности информации на платформе блокчейн.
122. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей
123. Методика инвентаризации, классификации и анализа информационных активов организации.
124. Методика генерации сценариев целевых атак на информационные системы
125. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персонала и степени их дублирования.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

6.1 Печатные и электронные издания

1. Федеральный Закон РФ №5485-1 1993 года «О государственной тайне».
2. Федеральный Закон РФ № 149-ФЗ 2006 года «Об информации, информационных технологиях и защите информации».
3. Федеральный Закон РФ №63-ФЗ 2011 года «Об электронной подписи».
4. Федеральный Закон РФ № 98-ФЗ 2004 года «О коммерческой тайне».
5. Федеральный Закон РФ № 152-ФЗ 2006 года «О персональных данных».
6. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.
7. Федеральный закон «О техническом регулировании» от 27.12.2002 г. №ФЗ-184
8. Указ Президента РФ № 1203 1995 года «Об утверждении Перечня сведений, отнесенных к государственной тайне».
9. Указ Президента РФ № 188 1997 года «Об утверждении Перечня сведений конфиденциального характера».
10. Постановление правительства Российской Федерации от 8 февраля 2018 г. N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

11. Стандартизация в Российской Федерации. Основные положения. Национальный стандарт РФ. ГОСТ Р 1.0 – 2012. – М.: Стандартинформ, 2013., [Электронный документ], <http://meganorm.ru/Index/53/53710.htm>.
12. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27002-2012. – М.: Стандартинформ, 2014., [Электронный документ], <http://meganorm.ru/Index/54/54705.htm>.
13. Защита информации. Система стандартов. Основные положения. Национальный стандарт РФ ГОСТ Р 52069.0-2013. – М.: Стандартинформ, 2014., [Электронный документ], <http://meganorm.ru/Index/54/54319.htm>.
14. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 15408-1-2012. – М.: Стандартинформ, 2014., [Электронный документ], <http://meganorm.ru/Index/54/54198.htm>.
15. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 15408-2-2013. – М.: Стандартинформ, 2014., [Электронный документ], <http://meganorm.ru/Index/55/55439.htm>.
16. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 15408-3-2013. – М.: Стандартинформ, 2014., [Электронный документ], <http://meganorm.ru/Index/55/55440.htm>.
17. СТО 56947007-25.040.40.227-2016 Типовые технические требования к функциональной структуре автоматизированных систем управления технологическими процессами подстанций Единой национальной электрической сети (АСУ ТП ПС ЕНЭС).
18. СТО 56947007-25.040.40.226-2016 Общие технические требования к АСУ ТП ПС ЕНЭС. Основные требования к программно-техническим средствам и комплексам.
19. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Стандарт Банка России. СТО БР ИББС-1.0-2014, [Электронный документ], http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf.
20. ГОСТ Р МЭК 60870-5-101-2006 Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 101
21. ГОСТ 2.102-2013. Виды и комплектность конструкторских документов.
22. ГОСТ Р МЭК 60870-5-104-2004 МЭК 60870-5-104:2000 "Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 104. Доступ к сети для МЭК 870-5-101 с использованием стандартных транспортных профилей
23. Протокол Modbus TCP (MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE)
24. Серия стандартов СТО 56947007-33.040.20.290-2019
25. СТО 56947007-25.040.40.112-2011 Типовая программа и методика испытаний программно-технического комплекса автоматизированной системы управления технологическими процессами (ПТК АСУ ТП) и микропроцессорного комплекса системы сбора и передачи информации (МПК ССПИ) подстанций в режиме повышенной информационной нагрузки «шторм».
26. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности
27. ИЕС 61850-8-1: Описание специфического сервиса связи (про запросу)
28. ГОСТ 24.104-85. Автоматизированные системы управления

29. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования".

30. Приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

31. Приказ ФСТЭК России от от 14 марта 2014 г. N 31 «Об утверждении Требований по обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

32. Приказ ФСТЭК России от от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных».

33. Приказ ФСТЭК России 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

34. Минзов А.С., Мещерский В.А. и др. Разработка концепции создания научно-образовательного центра защиты информации в корпоративных информационных системах и его научного, организационного, материального и кадрового обеспечения на базе Международного университета «Дубна»/ Отчет о научно-исследовательской работе - Дубна: Изд-во Межд. Университета «Дубна», 2019.

35. Минзов А.С. Профессиональная этика специалиста в сфере информационной и экономической безопасности: Монография/ А.С.Минзов. – М.:Изд-во ВНИИГеосистем, 2013. –150 с.

36. Минзов А.С. Формирование профессиональных компетенций в сфере защиты информации с использованием деловых игр / Тези доповідей Четвертої науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації" м.Вінниця, 23-25 квітня 2013 року. - Вінниця:ПП ТД "Едельвейс і К", 2013. -386-388с.

37. Минзов А.С., Мельникова О.И., Григорьев Д.С. Моделирование угроз экономической безопасности в системах дистанционного обучения/ Статья в сборник трудов Международной научно-методическая конференция «Информатизация инженерного образования».-М.: Национальный исследовательский университет «МЭИ», 2014 г.

38. Минзов А.С., Токарева Н.А., Торосян Ш.Г. Защита авторских прав в системах электронного обучения/ Статья в сборник трудов Международной научно-методическая конференция «Информатизация инженерного образования».-М.: Национальный исследовательский университет «МЭИ», 2014 г.

39. Minzov A., Tokareva N., Torosyan Sh. ON THE PROBLEM OF COPYRIGHT PROTECTION ON THE INTERNET/ Innovative Information Technologies: Materials of the International scientific –Practical conference. Part 1. /Ed. Uvaysov S. U.–M.: HSE, 2014, 349-354 p.

40. Minzov A., O.I.Melnikova, D.S. Grigoryev SOME APPROACHES OF MODELING THE THREAT TO ECONOMIC SECURITY OF THE MANAGING SUBJECT/ Innovative Information Technologies: Materials of the International scientific –Practical conference. Part 1. /Ed. Uvaysov S. U.–M.: HSE, 2014, 354-357 p

41. Минзов А.С., Мельникова О.И., Токарева Н.А., Бушеленкова С.В., Карпова М.А. О некоторых подходах к разработке эффективных систем экономической безопасности/ Вестник Международного университета природы, общества и человека «Дубна» /Серия «Системный анализ в современном обществе» №1 (29), 2014 г.

42. Минзов А.С., Мельникова О.И. О НЕКОТОРЫХ ПОДХОДАХ К РЕШЕНИЮ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУТП ОБЪЕКТОВ ТЕПЛОВОЙ И ГИДРО- ЭЛЕКТРОЭНЕРГЕТИКИ ОТ КИБЕРУГРОЗ /Сб. трудов Международной конференции «Инновации на основе информационных и коммуникационных технологий» (Адлер 1-10 октября 2014 г.) № 1. С. 484-485.
43. Минзов А.С., Невский А.Ю. ПРОБЛЕМЫ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ/ статья в сборник Известия КГТУ им. И. Раззакова, стр.504—507, 2014 г.
44. Аракелян Э.К., Минзов А.С. Особенности информационной безопасности АСУТП электростанций на базе современных программно-технических комплексов/ совместный доклад на конференции «Информационная безопасность АСУ ТП КВО» 4-5 февраля 2014 года, Москва.
45. Минзов А.С. Принципы создания эффективных систем экономической безопасности/ XI Международная научно-практическая конференция "Теория и практика экономики и предпринимательства" /доклад на Международной конференции 24-26 апреля 2014 Ялта (Гурзуф).
46. Аракелян Э.К., Андрияшин А.В., Минзов А.П. Особенности систем информационной безопасности АСУТП ТЭС и АЭС /статья в журнал Вестник БГУИР (Беларусь), стр.213-215, 2014 г.
47. Аракелян Э.К., Андрияшин А.В., Минзов А.П., Мезин С.В. Проблемы информационной безопасности АСУТП ТЭС и АЭС и возможные подходы к их решению/ статья в журнал «Новое в электроэнергетике», 2015 г.
48. Минзов А.С., Невский А.Ю., Баронов О.Р., Унижаев Н.В. Некоторые подходы к формированию профессиональных компетенций в сфере информационной безопасности/ статья в сборник трудов XIV Международной научно-практической конференции «Информационная безопасность» и заседания Южного регионального отделения учебно-методического объединения по образованию в области информационной безопасности, г.Таганрог, 3-7 июня 2015 г.
49. Minzov A.S, Baronov O.R., Melnikova O.I. SOME APPROACHES TO THE PROTECTION OF AUTOMATED CONTROL SYSTEMS FROM CYBERTHREATS/ Innovative Information Technologies: Materials of the International scientific –Practical conference. Part 1. /Ed. Uvaysov S. U.–M.: HSE, 2015.
50. Minzov A., Baronov O.R., Chukhrov A.A. ANTI-FRAUD MECHANISMS IN ENERGY COMPANIES/ Innovative Information Technologies: Materials of the International scientific –Practical conference. Part 1. /Ed. Uvaysov S. U.–M.: HSE, 2015.
51. Минзов А.С., Невский А.Ю., Баронов О.Р., Унижаев Н.В. О проблемах развития учебно-материальной базы в сфере информационной безопасности/ доклад на заседании Южного регионального отделения учебно-методического объединения по образованию в области информационной безопасности, г. Таганрог, 2015 г.
52. Минзов А.С., Торосян Ш.Г., Черемисина Е.Н., Чухров А.А. НОВЫЕ ПОДХОДЫ К ПРЕДУПРЕЖДЕНИЮ УТЕЧЕК ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ/ статья в сборник трудов XI Международной научно-практической конференции «Инновации на основе информационных и коммуникационных технологий».-Сочи (Адлер), 1-10 сентября 2015 г.
53. Минзов А.С., Седов Д.Д., Черемисина Е.Н., Чухров А.А. МЕХАНИЗМЫ ВЫЯВЛЕНИЯ СИСТЕМЫ ПРЕДПОЧТЕНИЙ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ ИНТЕРНЕТ/ статья в сборник трудов XI Международной научно-практической конференции «Инновации на основе информационных и коммуникационных технологий».-Сочи (Адлер), 1-10 сентября 2015 г.
54. Master SCADA. Основы проектирования. Руководство пользователя. – М.: ИнСАР, 2014. – 186 с."

55. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи, ДМК Пресс, 2005.
56. Марусина М.Я. и др. Основы метрологии, стандартизации и сертификации. – СПб.: СПбГУ ИТМО, 2009.
57. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 27001-2006. – М.: Стандартинформ, 2008.
58. Защита информации. Основные термины и определения. Национальный стандарт РФ. ГОСТ Р 50922-2006. – М.: Стандартинформ, 2008., [Электронный документ], <http://meganorm.ru/Index/5/5737.htm>.
59. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Государственный стандарт СССР. ГОСТ 28147 – 89. – М., ИПК Издательство стандартов, [Электронный документ], <http://meganorm.ru/Index/11/11287.htm>.
60. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Национальный стандарт РФ. ГОСТ Р 34.10-2012. – М.: Стандартинформ, 2013., [Электронный документ], <http://meganorm.ru/Data2/1/4293788/4293788463.pdf>.
61. Информационная технология. Криптографическая защита информации. Функции хэширования. Государственный стандарт РФ. ГОСТ Р 34.11-2012. – М.: Стандартинформ, 2013., [Электронный документ], <http://meganorm.ru/Data2/1/4293788/4293788459.pdf>.
62. Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. ГОСТ Р ИСО/МЭК ТО 15446-2008. М.: Стандартинформ, 2010., [Электронный документ], <http://meganorm.ru/Index/48/48618.htm>.
63. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60х90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378- 6 - Режим доступа: <http://znanium.com/catalog/product/474838>.
64. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - М.:Форум, НИЦ ИНФРА-М, 2015. - 352 с.: 60х90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: <http://znanium.com/catalog/product/489084>.
65. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — www.dx.doi.org/10.12737/11380. - Режим доступа: <http://znanium.com/catalog/product/763644>.
66. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60х88 1/16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379- 3 - Режим доступа: <http://znanium.com/catalog/product/549914>.
67. Комплексная система защиты информации на предприятии: учебное пособие для вузов по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации" / Н. В. Гришина. – М.: Форум, 2013. – 240 с. – (Профессиональное образование). - ISBN 978-5-91134-369-9.
68. Защита конфиденциальной информации: учебное пособие для вузов по специальностям 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мещатунян. – М.: Форум, 2013. – 256 с. – (Высшее образование). - ISBN 978-5-91134-336-1.
69. Комплексная защита информации в корпоративных системах: учебное пособие для вузов по направлению "Информатика и вычислительная техника" / В. Ф.

Шаньгин. – М.: Форум: ИНФРА-М, 2013. – 592 с. – (Высшее образование). - ISBN 978-5-8199-0411-4

70. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. 272 с.: ил. - (Серия «Библиотека программиста»). https://codernet.ru/books/hacking/audit_bezопасnosti_informacionnyh_sistem/.

71. Федотов Н.Ф. Форензика – компьютерная криминалистика. – М. «Onebook.ru», 2013. – 420 с.: ил. <https://forensics.ru/>.

72. Петренко С. А., Петренко А. А. Аудит безопасности Intranet. – М.: «ДМК Пресс». – 386 с.: ил. (Информационные технологии для инженеров). <https://static.my-shop.ru/product/pdf/89/886743.pdf>.

73. Аверченков В.И. Аудит информационной безопасности, - учеб. пособие для вузов – 3-е издание. М.: «ФЛИНТА», 2016. – 269 с. <https://avidreaders.ru/read-book/audit-informacionnoy-bezопасnosti-uchebnoe-posobie.html>.

74. Под общей редакцией Курило А.П. Аудит информационной безопасности. – М. Издательская группа «БДЦ-пресс», 2006. – 304 с.: ил.

6.2 Лицензионное и свободно распространяемое программное обеспечение: ОС Windows, Microsoft Office.

6.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

Университетская информационная система «РОССИЯ» <https://uisrussia.msu.ru>

Справочно-правовая система «Консультант+» <http://www.consultant-urist.ru>

Справочно-правовая система «Гарант» <http://www.garant.ru>

База данных Web of Science <https://apps.webofknowledge.com/>

База данных Scopus <https://www.scopus.com>

Портал открытых данных Российской Федерации <https://data.gov.ru>

База открытых данных Министерства труда и социальной защиты РФ <https://rosmintrud.ru/opendata>

База данных Научной электронной библиотеки eLIBRARY.RU <https://elibrary.ru/>

База данных профессиональных стандартов Министерства труда и социальной защиты РФ <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>

Базы данных Министерства экономического развития РФ <http://www.economy.gov.ru>

База открытых данных Росфинмониторинга <http://www.fedsfm.ru/opendata>

Электронная база данных «Издательство Лань» <https://e.lanbook.com>

Федеральная государственная информационная система «Национальная электронная библиотека» <https://нэб.рф>

Национальный портал онлайн обучения «Открытое образование» <https://openedu.ru>

Электронная база данных "Polpred.com Обзор СМИ" <https://www.polpred.com>

Официальный сайт Федерального агентства по техническому регулированию и метрологии <http://protect.gost.ru/>

Электронная библиотека МЭИ <https://ntb.mpei.ru/e-library/index.php>

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Для проведения государственной итоговой аттестации необходимо наличие учебной аудитории и помещение для самостоятельной работы обучающихся.