

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

---

**Направление подготовки/специальность: 10.04.01 Информационная безопасность**

**Наименование образовательной программы: Управление информационной безопасностью**

**Уровень образования: магистратура**

**Форма обучения: очная**

**Программа**  
**ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**


<b>Блок</b>	<b>Блок 3 «Государственная итоговая аттестация»</b>
<b>Трудоемкость в зачетных единицах</b>	<b>4 семестр – 6</b>
<b>Часов (всего) по учебному плану</b>	<b>216</b>
включая:  подготовку к сдаче и сдачу государственного экзамена  подготовку к процедуре защиты и процедуру защиты выпускной квалификационной работы	учебным планом не предусмотрены  4 семестр – 216 часов

**Москва 2021**

## ПРОГРАММУ СОСТАВИЛ:

Профессор кафедры безопасности и  
информационных технологий, д.т.н.,  
профессор

(должность, ученая степень, ученое звание)

  
(подпись)

А.С. Минзов

(расшифровка подписи)

Заведующий кафедрой безопасности и  
информационных технологий

(название кафедры)

  
(подпись)

А.Ю. Невский

(расшифровка подписи)

Руководитель образовательной программы

Профессор кафедры безопасности и  
информационных технологий, д.т.н.,  
профессор

(должность, ученая степень, ученое звание)

  
(подпись)

А.С. Минзов

(расшифровка подписи)

Руководитель научного содержания программы

Профессор кафедры безопасности и  
информационных технологий, д.т.н.,  
профессор

(должность, ученая степень, ученое звание)

  
(подпись)

А.П. Еремеев

(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 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455, зарегистрированным в Минюсте России 18.02.2021 г., регистрационный номер 62549 и профессиональных стандартов:
  - 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;

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

В результате освоения образовательной программы у выпускника должны быть сформированы следующие компетенции:

### 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 критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД-1 <sub>УК-1</sub> . Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи ИД-2 <sub>УК-1</sub> . Анализирует проблемную ситуацию и осуществляет ее декомпозицию на отдельные задачи ИД-3 <sub>УК-1</sub> . Вырабатывает стратегию решения поставленной задачи
разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	ИД-1 <sub>УК-2</sub> . Участвует в управлении проектом на всех этапах жизненного цикла
командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИД-1 <sub>УК-3</sub> . Демонстрирует понимание принципов командной работы ИД-2 <sub>УК-3</sub> . Руководит членами команды для достижения поставленной цели
коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для	ИД-1 <sub>УК-4</sub> . Осуществляет академическое и профессиональное взаимодействие, в том числе на иностранном языке ИД-2 <sub>УК-4</sub> . Переводит академические

	академического профессионального взаимодействия	и тексты (рефераты, аннотации, обзоры, статьи и т.д.) с иностранного языка или на иностранный язык ИД-3 <sub>УК-4</sub> . Использует современные информационно-коммуникативные средства для коммуникации
межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	ИД-1 <sub>УК-5</sub> . Демонстрирует понимание особенностей различных культур и наций ИД-2 <sub>УК-5</sub> . Выстраивает социальное взаимодействие, учитывая общее и особенное различных культур и религий
самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИД-1 <sub>УК-6</sub> . Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания ИД-2 <sub>УК-6</sub> . Определяет приоритеты личностного роста и способы совершенствования собственной деятельности на основе самооценки

## 2.2. Общепрофессиональные компетенции выпускников

Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИД-1 <sub>ОПК-1</sub> . Самостоятельно осваивает и адаптирует к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты ИД-2 <sub>ОПК-1</sub> . Организовать управление информационной безопасностью
	ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИД-1 <sub>ОПК-2</sub> . Анализирует угрозы информационной безопасности объектов и разрабатывать методы противодействия им
	ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИД-1 <sub>ОПК-3</sub> . Организует работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России ИД-2 <sub>ОПК-3</sub> . Разрабатывает проекты организационно-распорядительных документов, бизнес-планов в сфере

		<p>профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, в том числе и на объектах энергетики с критической информационной инфраструктурой, использующих АСУ ТП</p> <p>ИД-3<sub>ОПК-3</sub>. Обосновывает и выполняет практические работы по организационному, техническому обеспечению безопасности информации в государственных информационных системах (ГИС)</p>
	ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	<p>ИД-1<sub>ОПК-4</sub>. Выполняет сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок</p> <p>ИД-2<sub>ОПК-4</sub>. Разрабатывает проект защиты информационных активов организации с использованием актуальной научно-технической информации и современных научных исследований</p>
	ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	<p>ИД-1<sub>ОПК-5</sub>. Проводит самостоятельные исследования в соответствии с разработанной программой и представлять их результаты в виде доклада или научной статьи</p> <p>ИД-2<sub>ОПК-5</sub>. Проводит экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента</p>

### 2.3. Профессиональные компетенции выпускников

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-1. Оценивание уровня безопасности компьютерных систем и сетей	<p>ПК-1.1<sub>ПК-1</sub>. Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации</p> <p>ПК-1.2<sub>ПК-1</sub>. Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей</p> <p>ПК-1.3<sub>ПК-1</sub>. Проводит анализ безопасности компьютерных систем</p> <p>ПК-1.4<sub>ПК-1</sub>. Проводит сертификацию программно-</p>

	<p>аппаратных средств защиты информации и анализ результатов</p> <p>ПК-1.5<sub>ПК-1</sub>. Проводит инструментальный мониторинг защищенности компьютерных систем и сетей</p> <p>ПК-1.6<sub>ПК-1</sub>. Проводит экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов</p>
ПК-2. Разработка систем защиты информации автоматизированных систем	<p>ПК-2.1<sub>ПК-2</sub>. Тестирует системы защиты информации автоматизированных систем</p> <p>ПК-2.2<sub>ПК-2</sub>. Разрабатывает проектные решения по защите информации в автоматизированных системах</p> <p>ПК-2.3<sub>ПК-2</sub>. Разрабатывает эксплуатационную документацию на системы защиты информации автоматизированных систем</p>

### **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 4 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**

1. Управление событиями информационной безопасности в SIEM-системах.
2. Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ.
3. Использование системы мониторинга Zabbix в качестве сканера безопасности.
4. Реагирование на инциденты информационной безопасности в банковской сфере с использованием платформы «SECURITY VISION».
5. Технологии внедрения облачной электронной подписи в ЕАИС ФТС РОССИИ
6. Мониторинг политики сетевой безопасности на основе модели сценариев атак.
7. Проблема создания единой методологии гарантированной защиты информации для различных видов тайн.
8. Разработка способа мониторинга безопасности IoT-устройств на базе MQTT-брокера.
9. Оценка возможности создания единой методики защиты информации.
10. Моделирование процессов непрерывности бизнеса в информационной безопасности.

11. Оценка эффективности систем управления информационной безопасностью на имитационных моделях.
12. Повышение уровня доверия к технологии блокчейн с использованием подхода «Общих критериев».
13. Разработка описательных вариативных моделей объектов критической информационной инфраструктуры.
14. Разработка методики проведения теста на проникновение в информационные системы финансово-кредитных организаций на основе лучших практик.
15. Разработка научно-методического обеспечения обучения администрированию безопасности операционных систем.
16. Разработка алгоритмов и методик оценки эффективности систем обеспечения информационной безопасности на имитационных моделях
17. Разработка методики проведения выявления и расследования инцидентов утечки информации в корпоративных информационных системах с использованием DLP-систем.
18. Моделирование процессов влияния алгоритмов обработки информации на побочные электромагнитные излучения в ПЭВМ.
19. Моделирование и оценка уровня ПЭМИ для стационарных компьютеров организационно-техническими методами.
20. Применение технологий проактивной защиты SIEM при мониторинге событий информационной безопасности.
21. Проактивные системы информационной безопасности и особенности их применения в корпоративных информационных системах.
22. Научно-методическое обеспечение для обучения технологиям тестирования безопасности прикладного программного обеспечения, используемого в WEB-сервисах.
23. Научно-методическое обеспечение аудита информационной безопасности информационных систем.
24. Научно-методическое обеспечение обучения методам и технологиям администрирования сетевого оборудования в защищенных информационных системах.
25. Научно-методическое обеспечение обучения технологиям создания удостоверяющего центра на основе OpenSSL.
26. Научно-методическое обеспечение применения механизмов защиты конфиденциальной речевой информации в сегменте корпоративной сети VOIP.
27. Научно-методическое обеспечение защиты коммерческой тайны в корпоративной информационной системе.
28. Научно-методическое обеспечение расследования инцидентов информационной безопасности информационных систем.
29. Научно-методическое обеспечение обучения технологиям защиты информационных систем от кибератак в формате “attack-defense”.
30. Научно-методическое обеспечение для обучения технологиям криптографической защиты информации.

## **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 АСУТП 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](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 «штурм».

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.–М.: 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.– М.: 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.: ИнСАТ, 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](http://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](http://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/](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.myshop.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.