

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: Организация и технология защиты информации

Уровень образования: бакалавриат

Форма обучения: очная


Программа
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Блок	Блок 1 «Дисциплины (модули)»
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 и профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464); Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

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

2.1. Общекультурные (универсальные) компетенции

Выпускник, освоивший образовательную программу, должен обладать следующими общекультурными компетенциями (ОК):

- 1) способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- 2) способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- 3) способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
- 4) способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- 5) способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- 6) способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- 7) способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
- 8) способностью к самоорганизации и самообразованию (ОК-8);
- 9) способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

2.2. Общепрофессиональные компетенции

Выпускник, освоивший образовательную программу, должен обладать следующими общепрофессиональными компетенциями (ОПК):

- 1) способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);
- 2) способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

3) способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

4) способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

5) способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

6) способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

7) способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

2.3. Профессиональные компетенции

Выпускник, освоивший образовательную программу, должен обладать профессиональными компетенциями, соответствующими виду (видам) профессиональной деятельности, на который (которые) ориентирована образовательная программа:

При осуществлении эксплуатационной деятельности:

1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

3) способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

4) способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

5) способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

6) способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6).

При осуществлении проектно-технологической деятельности:

1) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

2) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8).

При осуществлении экспериментально-исследовательской деятельности:

1) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

2) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

3) способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

4) способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

При осуществлении организационно-управленческой деятельности:

1) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

2) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

3) способностью организовывать 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 (ПК-15).

2.4. Профессионально-специализированные компетенции (выпускник должен обладать):

1) способностью администрировать подсистемы информационной безопасности объектов, включая объекты энергетики КВО РФ, эксплуатирующие АСУ ТП (ПСК-1);

2) способностью применять программные средства системного, прикладного и специального назначения, в том числе для обеспечения безопасного функционирования объектов энергетики с элементами АСУ ТП (ПСК-2);

3) способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП (ПСК-3).

1. 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 защита выпускной квалификационной работы.

2. КРАТКОЕ СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИН, ВКЛЮЧЕННЫХ В ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН

Государственный экзамен учебным планом не предусмотрен.

3. ПРИМЕРНАЯ ТЕМАТИКА ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

1. Защита персональных данных финансово-кредитной организации
2. Защита персональных данных в коммерческой организации
3. Защита персональных данных в организации с участием государства (муниципальном образовании)
4. Защита персональных данных в медицинских учреждениях
5. Защита электронного документооборота на предприятии
6. Инвентаризация информационных активов организации

7. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере организации малого (среднего) бизнеса)
8. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере финансово-кредитного учреждения)
9. Защита коммерческой тайны в организации
10. Защита информации в концепции стандарта ГОСТ Р 27001-2006 (на примере общественной организации)
11. Защита информации в концепции стандарта COBIT 5.0 (на примере некоммерческой организации)
12. Защита служебной тайны в организации
13. Защита интеллектуальной собственности в организации
14. Сертификация СМИБ по стандарту ГОСТ Р ИСО/МЭК 27001
15. Аттестация системы информационной безопасности государственной информационной системы
16. Разработка модели угроз информационной безопасности в финансово-кредитном учреждении
17. Разработка модели нарушителя информационной безопасности в организации
18. Разработка модели нарушителя информационной безопасности в организации, относящейся к критической информационной инфраструктуре
19. Разработка программного обеспечения выделения агрегатов рисков по общим угрозам, уязвимостям и активам
20. Имитационное моделирование сценариев рисков информационной безопасности
21. Анализ рисков информационной безопасности в информационной системе персональных данных
22. Мониторинг состояния объекта на основе оценки рисков
23. Автоматизированный выбор мер и средств контроля и управления по заданным рискам с использованием нейронных сетей
24. Моделирование рисков информационной безопасности в информационных системах, построенных по технологии блокчейн
25. Инвентаризация и классификация информационных активов организации при оценке рисков
26. Оценка и анализ рисков с использованием программного обеспечения CORAS
27. Организация режима защиты конфиденциальной информации на предприятии государственного сектора экономики
28. Разработка комплекта документации по результатам аттестации объекта информатизации (автоматизированной системы)
29. Разработка политики информационной безопасности организации
30. Разработка комплекса мероприятий по лицензированию деятельности предприятия по технической защите конфиденциальной информации
31. Разработка комплекса мероприятий по сертификации средства обработки конфиденциальной информации
32. Разработка комплекса мероприятий по сертификации средства защиты информации
33. Организация режима коммерческой тайны на предприятии
34. Разработка частных политик информационной безопасности для организации
35. Моделирование угроз персональным данным в организации
36. Обеспечение безопасности информации на объектах критической информационной инфраструктуры
37. Документальное обеспечение режима коммерческой тайны предприятия
38. Формирование требований к сотруднику службы информационной безопасности при внедрении профессиональных стандартов

39. Разработка и реализация программы повышения осведомленности сотрудников предприятия (организации) в области информационной безопасности
40. Организация проверки и оценки уровня подготовки персонала предприятия, участвующего в обработке конфиденциальной информации
41. Управление поведением персонала при организации безопасной работы в информационной системе организации
42. Инструментальные проверки персонала организации, использующего в работе конфиденциальную информацию
43. Подготовка персонала организации, использующего в работе конфиденциальную информацию с использованием дистанционных образовательных технологий
44. Организация расследования инцидентов информационной безопасности на предприятии
45. Обеспечение режима конфиденциальности в организации при увольнении сотрудников
46. Организация специальных инструментальных проверок персонала для противодействия инсайдерству в финансовом учреждении (на предприятии энергетики)
47. Разработка проекта технической защиты конфиденциальной информации на предприятии от ее утечки по (конкретный вид) каналу
48. Разработка проекта технической защиты информации на автоматизированном рабочем месте от ее утечки по (конкретный вид) каналу
49. Проектирование системы охранного видеонаблюдения организации с использованием профессиональных графических инструментов
50. Разработка программы специального обследования по выявлению электронных устройств негласного получения информации в защищаемом помещении предприятия
51. Разработка программы специального обследования по выявлению временно отключенных электронных устройств негласного получения информации в защищаемом помещении предприятия
52. Разработка программы специального обследования защищаемого помещения (кабинета, переговорной комнаты, конференц-зала и т.д.) предприятия (организации)
53. Внедрение методов и способов организации автоматизированного пропускного режима на предприятии
54. Разработка технического проекта создания защищаемого помещения в организации
55. Разработка технического проекта системы защиты информации организации от утечки по постоянно действующим каналам связи
56. Разработка программы проведения специального обследования помещения организации по выявлению акустопараметрического канала утечки информации
57. Оценка защищенности планшетных компьютеров от утечки конфиденциальной информации по каналу ПЭМИ
58. Разработка проекта системы защиты конфиденциальной информации в организации
59. Разработка предложений по повышению защищенности вычислительной техники по каналу ПЭМИ пассивными методами
60. Разработка рекомендаций по защите конфиденциальной информации от утечки по акустическому каналу из защищаемого помещения пассивными методами
61. Разработка алгоритма поиска сигналов со сложными структурами в процессе радиомониторинга
62. Разработка технического задания на проведение поисковых работ по обнаружению скрытых неизлучающих устройств утечки информации

63. Автоматизация процесса подготовки отчетных документов по результатам проведения инструментального контроля уровня защищенности автоматизированного рабочего места
64. Администрирование систем безопасности сетевого взаимодействия на основе технологии VPN
65. Разработка комплекса правил, процедур и практических приемов защиты информации в мобильных устройствах
66. Программная защита информационной системы организации на основе возможностей операционной системы
67. Организация программной защиты сервера с использованием возможностей ОС Microsoft Windows
68. Разработка и внедрение электронной подписи в документооборот организации
69. Анализ уязвимостей систем удаленного видеонаблюдения на предприятии
70. Обеспечение безопасности сетевого взаимодействия с использованием технологии OpenVPN
71. Администрирование средств межсетевого экранирования в системе защиты информации организации
72. Применение межсетевых экранов экспертного уровня для защиты ресурсов локальной вычислительной сети в организации
73. Администрирование системы резервного копирования для защиты информационных активов организации
74. Внедрение в организации системы резервного копирования
75. Обеспечение безопасности сетевого взаимодействия с использованием технологии IPSec
76. Защита сетевого хранилища средствами QNAP NAS от несанкционированного доступа и нарушения целостности данных
77. Защита сетевого хранилища средствами Synology NAS от несанкционированного доступа и нарушения целостности данных
78. Организация программной защиты файлового сервера с использованием возможностей операционной системы AstraLinux
79. Организация программной защиты веб-сервера с использованием возможностей операционной системы AstraLinux
80. Организация программной защиты файлового сервера с использованием возможностей операционной системы ALT Linux
81. Организация программной защиты веб-сервера с использованием возможностей операционной системы ALT Linux
82. Администрирование программно-аппаратного комплекса «Соболь» на рабочих станциях в организации
83. Защита локальной вычислительной сети организации с использованием IDS/IPS систем
84. Диагностика стеганографических возможностей и противодействие им при реализации информационных процессов в организации
85. Разработка средств автоматизации для настройки средств защиты информации от несанкционированного доступа
86. Разработка средств автоматизации для контроля защищенности автоматизированных систем по требованиям безопасности информации
87. Разработка средств автоматизации для исследования программного обеспечения по требованиям безопасности информации
88. Разработка системы диагностики наличия вредоносного программного обеспечения («в локальной сети организации» или «на сетях IoT-устройств» или «в промышленной сети организации»)

89. Обеспечение безопасного подключения рабочих станций (название организации), обрабатывающих конфиденциальную информацию, к сети Интернет
90. 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)
91. Защита от несанкционированных проводных подключений к локальной сети (название организации)
- 92.
93. Организация аудита информационной безопасности организации с использованием специального программного обеспечения
94. Применение технологии активного аудита информационной безопасности в организации
95. Разработка программы проведения аудита информационной безопасности в организации
96. Разработка программы проведения внутреннего аудита информационной безопасности организации
97. Внедрение системы менеджмента инцидентов информационной безопасности в коммерческом банке
98. Организация мониторинга действий персонала организации с целью выявления инцидентов информационной безопасности
99. Внедрение технологий предотвращения утечки информации (DLP-системы) в организации
100. Внедрение технологии управления информацией и событиями безопасности (SIEM-системы) в организации
101. Автоматизация процессов менеджмента информационной безопасности в организации
102. Внедрение системы предотвращения утечки информации в финансово-кредитном учреждении
103. Внедрение системы сбора и корреляции событий информационной безопасности в финансово-кредитном учреждении
104. Организация центра управления информационной безопасностью в финансово-кредитном учреждении
105. Внедрение системы мониторинга информационной безопасности в финансово-кредитном учреждении
106. Расследование инцидентов информационной безопасности в организации
107. Проведение аудита информационной безопасности организации с использованием сканера безопасности
108. Аудит безопасности локальной вычислительной сети организации с использованием сканера безопасности
109. Защита информации с использованием методов и технологий упрощенной криптографии в организации
110. Криптографические способы контроля целостности и их практическая реализация
111. Асимметричные криптосистемы и методы обеспечения конфиденциальности при их использовании
112. Моделирование уязвимостей протоколов защиты TLS
113. Моделирование уязвимостей протоколов защиты SSL
114. Моделирование уязвимостей протоколов защиты информации в сетях Kerberos
115. Технология защиты авторских прав мультимедийных файлов с использованием цифровых водяных знаков

116. Обеспечение информационной безопасности Интернета вещей в цифровой экономике
117. Исследование механизмов целостности и доступности информации на платформе блокчейн.
118. Анализ технологий разработки смарт-контрактов и выявление их уязвимостей
119. Методика инвентаризации, классификации и анализа информационных активов организации.
120. Методика генерации сценариев целевых атак на информационные системы
121. Методика обоснования структуры службы информационной безопасности, функционального разделения обязанностей персонала и степени их дублирования.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

4.1. 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.

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.–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., Андриюшин 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., Андриюшин 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.: Стандартиформ, 2008.

58. Защита информации. Основные термины и определения. Национальный стандарт РФ. ГОСТ Р 50922-2006. – М.: Стандартиформ, 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. Мецатунян. – 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_bezopasnosti_informacionnyx_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-bezopasnosti-uchebnoe-posobie.html>.

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

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

4.3. 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>

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

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