



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»



УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храшкин

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ/НИР

ПРОИЗВОДСТВЕННАЯ - НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы

10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

| | |
|---------------------|---|
| Институт/ факультет | Институт энергетики и автоматизированных систем |
| Кафедра | Информатики и информационной безопасности |
| Курс | 6 |
| Семестр | 11 |

Магнитогорск
2026 год

Программа практики/НИР составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Программа практики/НИР рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
22.01.2026 протокол №5

Зав. кафедрой И.И. Баранкова И.И. Баранкова

Программа практики/НИР одобрена методической комиссией ИЭиАС
03.02.2026 г. Протокол № 5

Председатель В.Р. Храмшин В.Р. Храмшин

Программа составлена:

зав. кафедрой ИиИБ, д-р техн. наук И.И. Баранкова И.И. Баранкова

Рецензент:

Начальник отдела информационной безопасности "КУБ" (АО),

М.М. Блинецов М.М. Блинецов

Лист актуализации программы

Программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2031 - 2032 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2032 - 2033 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

1 Цели практики/НИР

Целями научно-исследовательской работы по специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин, приобретение и развитие необходимых умений и навыков в соответствии с требованиями к уровню подготовки выпускника.

2 Задачи практики/НИР

Задачами научно-исследовательской работы являются: формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение системы оценок эффективности применяемых мер обеспечения защиты информации.

3 Место практики/НИР в структуре образовательной программы

Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Методы проектирования систем защиты распределенных информационных систем

Защита программного обеспечения

Защита информационно-технологических ресурсов автоматизированных систем

Анализ безопасности информационных технологий

Форензика

Тестирование систем защиты информации автоматизированных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Моделирование систем защиты информации

Знания (умения, владения), полученные в процессе прохождения практики/НИР будут необходимы для изучения дисциплин/практик:

Производственная - преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

4 Место проведения практики/НИР

Способ проведения практики/НИР: нет

Практика/НИР осуществляется дискретно

5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения

В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями:

| Код индикатора | Индикатор достижения компетенции |
|----------------|--|
| ПК-1 | Способен проводить анализ безопасности компьютерных систем |
| ПК-1.1 | Оценивает эффективность защиты информации |
| ПК-1.2 | Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации |
| ПК-2 | Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей |
| ПК-2.1 | Разрабатывает профили защиты компьютерных систем |
| ПК-2.2 | Формирует политики безопасности компьютерных систем и сетей |

| | |
|--|---|
| ПК-3 Способен анализировать причины возникновения компьютерных инцидентов | |
| ПК-3.1 | Определяет причину и условия изменения программного обеспечения |
| ПК-3.2 | Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой |
| ПК-3.3 | Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов |
| ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей | |
| ПК-4.1 | Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем |
| ПК-4.2 | Применяет методы анализа защищенности компьютерных систем и сетей |
| ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации | |
| ПК-5.1 | Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации |
| ПК-5.2 | Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации |
| ПК-5.3 | Оформляет аттестат соответствия объектов вычислительной техники требованиям по защите информации |
| ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем | |
| ПК-6.1 | Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем |
| ПК-6.2 | Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем |
| ПК-6.3 | Выявляет основные угрозы безопасности информации в автоматизированных системах |
| ПК-6.4 | Составляет протоколы тестирования систем защиты информации автоматизированных систем |
| ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах | |
| ПК-7.1 | Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах |
| ПК-7.2 | Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы |
| ПК-7.3 | Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации |
| ПК-7.4 | Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем |

6. Структура и содержание практики/НИР

Общая трудоемкость практики/НИР составляет 15 зачетных единиц 540 акад. часов, в том числе:

- контактная работа – 6,1 акад. часов;
- самостоятельная работа – 533,9 акад. часов;
- в форме практической подготовки – 540 акад. часов.

| № п/п | Разделы (этапы) и содержание практики | Семестр | Виды работ на практике, включая самостоятельную работу | Код компетенции |
|-------|---|---------|--|--|
| 1. | Планирование научно-исследовательской работы, включающее ознакомление с тематикой исследовательских работ в области информационной безопасности, выбор темы исследования, подготовка литературного обзора | 11 | Ознакомление с тематикой исследовательских работ в области информационной безопасности, выбор темы исследования, подготовка литературного обзора | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-5.1, ПК-5.2, ПК-5.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4 |
| 2. | Проведение научно-исследовательской работы | 11 | Проведение научного исследования по выбранной тематике | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-5.1, ПК-5.2, ПК-5.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4 |
| 3. | Составление отчета о научно-исследовательской работе | 11 | Составление отчета о выполненной научно-исследовательской работе | ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-5.1, ПК-5.2, ПК-5.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4 |
| 4. | Защита выполненной работы | 11 | Представление доклада о выполненной НИР | |

7 Оценочные средства для проведения промежуточной аттестации по практике/НИР

Представлены в приложении 1.

8 Учебно-методическое и информационное обеспечение практики/НИР

а) Основная литература:

Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. <https://znanium.ru/catalog/document?id=477891&pid=957144> (дата обращения: 11.03.2026).

б) Дополнительная литература:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб.пособие для вузов / П.Н. Девянин .— 2-е изд., испр. и доп. — М. : Горячая линия – Телеком, 2013 .— 339 с. — ISBN 978-5-9912-0328-9 . — Режим доступа: <http://ibooks.ru/reading.php?productid=344413> (дата обращения: 11.03.2026).

2. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации: учебное пособие/Унижаев Н.В.–СПб.: Издательский центр «Интермедия», 2018.—408с. <https://ibooks.ru/reading.php?productid=356934> (дата обращения: 11.03.2026).

3. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие / Е.Г. Воробьев – СПб.: Издательский центр «Интермедия», 2016. —432 с. <https://ibooks.ru/reading.php?productid=351534> (дата обращения: 11.03.2026).

4. Царегородцев А. В., Тараскин М. М. Методы и средства защиты информации в государственном управлении : учебное пособие. — Москва : Проспект, 2017. — 208 с. <https://ibooks.ru/reading.php?productid=356008> (дата обращения: 11.03.2026).

5. Информационная безопасность при управлении техническими системами: учебное пособие / С.А. Баркалов, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов.—СПб : ИЦ «Интермедия», 2016. —528с.: илл. <https://ibooks.ru/reading.php?productid=356935> (дата обращения: 11.03.2026).

6. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. — 2017. - № 2. - С.25-34. DOI: 10.7256/2409-7543.2017.2.22065. URL: http://e-notabene.ru/nb/article_22065.html (дата обращения: 11.03.2026).

7. Коваленко, В. В. Проектирование информационных систем [Электронный ресурс]: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с. - (Высшее образование). –Режим доступа: <http://znanium.com/bookread.php?book=473097> .—Заглавие с экрана. —ISBN 978-5-91134-549-5 (дата обращения 11.03.2026).

8. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.- (Высшее образование).—Режим доступа: <http://znanium.com/bookread.php?book=402686> .—Заглавие с экрана. —ISBN 978-5-8199-0411-4 (дата обращения 11.03.2026).

9. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1858>

(дата обращения: 11.03.2026). - ISBN 978-5-9967-1031-7. - Текст : электронный*.

10. Разработка БД в MS SQL Server с использованием SSMS : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2021>. - ISBN 978-5-9967-1207-6. - Текст : электронный.

11. Разработка приложений на C# для работы с базами данных : практикум / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2317> (дата обращения: 11.03.2026). - Текст : электронный.

12. Теория информации. Кодирование : учебное пособие / И. И. Баранкова, М. В. Коновалов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1848> (дата обращения 11.03.2026). - ISBN 978-5-9967-1073-7. - Текст : электронный.

13. Техническая защита информации. Лабораторный практикум : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1747> (дата обращения: 11.03.2026). - Текст : электронный*.

14. Теория вероятностей : учебное пособие [для вузов] / Л. Л. Демиденко, Г. М. Коринченко ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2538>. - ISBN 978-5-9967-1653-1 (дата обращения 11.03.2026). - Текст : электронный.

15. Объектно-ориентированное программирование : учебное пособие / О. Б. Калугина, М. В. Надеина, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2015. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/308> (дата обращения 11.03.2026). - Текст : электронный.

16. Практикум по теории графов : практикум / О. Б. Калугина, Т. Н. Носова, Г. И. Лукьянов ; О. Б. Калугина, Т. Н. Носова, Г. И. Лукьянова ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1989> (дата обращения 11.03.2026). - Текст : электронный.

17. Практикум по математической статистике / В. В. Королева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2541> (дата обращения 11.03.2026). - Текст : электронный.

18. Создание классов в C#: интерактивный справочно-обучающий практикум : практикум / Т. Н. Носова ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/ToView/20750?idb=db0109> (дата обращения 11.03.2026). - Текст : электронный.

19. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] / [сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2388> (дата обращения 11.03.2026). - ISBN 978-5-9967-1305-9. - Текст : электронный*.

20. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева ;

Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://host.megaprolib.net/MP0109/Download/MObject/2400> (дата обращения 11.03.2026). - ISBN 978-5-9967-1605-0. - Текст : электронный*.

21. Теория графов и ее приложения : учебное пособие / О. Б. Калугина, В. В. Баранкова, Т. Н. Носова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1908> (дата обращения 11.03.2026). - ISBN 978-5-9967-1078-2. - Текст : электронный.

в) Методические указания:

Представлены в приложениях

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

| Наименование ПО | № договора | Срок действия лицензии |
|------------------|------------------------------|------------------------|
| MS Office 2007 | № 135 от 17.09.2007 | бессрочно |
| MathCAD v.15 | Д-1662-13 от 22.11.2013 | бессрочно |
| LibreOffice | свободно распространяемое ПО | бессрочно |
| Borland Turbo | №112301 от 23.11.2005 | бессрочно |
| Borland Turbo | №112301 от 23.11.2005 | бессрочно |
| MS Visual Studio | свободно распространяемое ПО | бессрочно |
| MS Visual Studio | свободно распространяемое ПО | бессрочно |
| Adobe Reader | свободно распространяемое ПО | бессрочно |
| СЗИ Страж NT | К-271-12 от 16.10.2012 | бессрочно |
| СКЗИ КриптоПро | К-271-12 от 16.10.2012 | бессрочно |
| VIP Net Client | Д-946-14 от 22.07.2014 | бессрочно |
| VIP Net | Д-946-14 от 22.07.2014 | бессрочно |
| Браузер Yandex | свободно распространяемое ПО | бессрочно |
| Браузер Mozilla | свободно распространяемое ПО | бессрочно |
| FAR Manager | свободно распространяемое ПО | бессрочно |
| Linux Calculate | свободно распространяемое ПО | бессрочно |

9 Материально-техническое обеспечение практики/НИР

Рабочее место обучающегося при прохождении практики должно соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

Обучающимся должна быть обеспечена возможность доступа к информации, необходимой для выполнения задания по практике и написанию отчета.

Организации, учреждения и предприятия, а также учебно-научные подразделения Университета должны обеспечить рабочее место обучающегося компьютерным оборудованием в объемах, достаточных для достижения целей практики.

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки) оснащены персональными компьютерами с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета».

Материально-техническое обеспечение учебной практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности включает:

Комплекс радиомониторинга «Касандра К-6».

Комплекс радиомониторинга «Касандра К-21».

Анализатор спектра «АКС-1301».

Комплект оборудования для мониторинга информационной безопасности.

Комплект оборудования контроля доступа.

Комплект оборудования для построения сети ZigBee.

Комплект оборудования SECURITY-CISCO-3М.

Портативный поисковый комплекс амплитудной пеленгации «Касандра Сб»

Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Программно-аппаратный комплекс для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи Лазурит

Фильтр сетевой помехоподавляющий «ЛФС-100-3Ф»

Генератор шума ГШ-1000М.

Соната-АВ (модель 3М) система виброакустической и акустической защиты (Центральный ГШ): Генераторный блок (Модель 3М) + Аудиоизлучатель АИ-3М + «Тяжелый» виброизлучатель ВИ-3М + «Легкий» виброизлучатель ПИ-3М.

Устройство защиты Прокруст 2000.

Устройство КРИПТОН-ЗАМОК/У (АПМДЗ-У, М-526Б).

Устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2» исп. 208.

Комплект оборудования «Беспроводные компьютерные сети ЭВМ».

Модуль «Низкоуровневый контроллер Ethernet»

Комплект коммуникационного оборудования с сервером для моделирования облачного сервиса

Электронные ключи Guardant, eToken.

Комплект оборудования пользовательского сегмента системы GPS.

Комплект оборудования ТЛС-1.

Комплект оборудования VOIP.

Комплект оборудования «Кодирование и модуляция информации в системах связи».

Комплект оборудования «Исследование дистанционной передачи информации»

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация по научно-исследовательской работе имеет целью определить степень достижения запланированных результатов обучения и проводится в форме зачета с оценкой.

Обязательной формой отчетности обучающегося по НИР является письменный отчет. Цель отчета – сформировать и закрепить компетенции, приобретенные обучающимся в результате освоения теоретических курсов и полученные им при выполнении НИР.

Уровень знаний определяется следующими оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– на оценку «отлично» – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «хорошо» – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку «удовлетворительно» – обучающийся прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку «неудовлетворительно» – обучающийся не прошел запланированные рубежные контроли и не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

Примерный перечень вопросов на защите отчета НИР:

1. Какая научно-исследовательская задача решалась в ходе выполнения НИР?
2. Какие методы исследования применялись при выполнении НИР?
3. Как тема исследовательской работы согласовывается со списком приоритетных направлений развития науки и техники в РФ?
4. Какими нормативно правовыми актами регулируется информационная безопасность на объекте исследований?
5. Существуют ли отечественные и зарубежные аналоги объекта научных исследований?
6. Укажите области применения предложенной Вами разработки?
7. Оцените экономический эффект от внедрения Вашей разработки в отрасли экономики РФ?
8. Какими способами осуществлялась проверка достоверности полученных результатов?
9. Какие инновационные решения были разработаны в ходе выполнения НИР?
10. Какие охранные документы были получены в ходе выполнения НИР?

Задачами НИР также являются участие обучающихся в научных всероссийских и международных конференциях и публикации статей и докладов по результатам исследования.

Примерный перечень тем докладов и публикаций обучающихся:

- Разработка модуля подавления 5G сетей
- Разработка портативного модуля для определения скрытых закладок в USB устройствах
- Анализ безопасности спецификации протокола высокого уровня ZIGBEE
- Кибербезопасность АСУ ТП предприятий Индустрии 4.0
- Организация защиты персональных данных
- Потребителей интернет вещей с помощью урегулирования их отношений на законодательном уровне
- Использование искусственных отпечатков пальцев для взлома биометрической системы защиты
- Использование особых точек отпечатков пальцев в биокриптографии и кодировании информации
- Анализ математической модели комплекса радиомониторинга для повышения эффективности оценки защищенности
- Использование возможностей комплекса радиомониторинга «Кассандра» для обнаружения современных технических средств с передачей информации по радиоканалу
- Разработка виртуального тренажёра для оценки защищенности акустической информации в контролируемом помещении
- Применение стеганографии для формирования архивов данных
- Практика применения обфускации программного кода
- Анализ уязвимостей АСУ ТП как объекта критической информационной инфраструктуры
- Принципы построения модели надежности системы управления кибербезопасностью АСУ ТП

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.6) «Оценочные средства для проведения промежуточной аттестации» данной РПД.