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
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ/НИР

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

Направление подготовки (специальность)
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	10

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности «КУБ» (АО)

_____ М.М. Близнецов

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:

Анализ рисков информационной безопасности

Методы мониторинга информационной безопасности АС

Методы проектирования защищенных распределенных информационных систем

Моделирование систем и процессов защиты информации

Управление информационной безопасностью

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

Подготовка к защите и защита выпускной квалификационной работы

Производственная-преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

4 Место проведения практики/НИР

Способ проведения практики/НИР: выездная и/или стационарная

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:

Структурный элемент компетенции	Планируемые результаты обучения
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	

Знать	- нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. - порядок разработки модели угроз − цели и задачи моделирования систем и процессов защиты информации; - способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем
Уметь	- обосновать выбор подходящего метода и привести алгоритм решения задачи; - формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения - применять новые технологии проектирования и анализа систем - проводить мониторинг угроз безопасности информационных систем
Владеть	- навыками решения моделирования процессов защиты информации - навыками проектирования информационных структур - навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; − навыками анализа основных узлов и устройств современных автоматизированных систем
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Этапы создания междисциплинарных и инновационных проектов.
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов

ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	
Знать	Основы построения систем обработки и передачи информации, их современное состояние развития. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. Особенности обработки информации с использованием компьютерных систем
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.
Владеть	Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам. Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.
ПК-2 способностью создавать и исследовать модели автоматизированных систем	
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах
Уметь	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации − анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем

Владеть	-навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей -навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
Знать	источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
Уметь	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
Владеть	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	
Знать	нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов
Уметь	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	способностью разрабатывать научно-техническую документацию
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	

Знать	Средства анализа информационной безопасности; Классификацию систем защиты информации; Средства организации аттестации ВП по требованиям безопасности информации.
Уметь	Принимать участие в исследованиях аттестации системы защиты информации; Принимать участие в исследованиях и анализе аттестации системы защиты информации; Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.
Владеть	Навыками использования средств анализа информационной безопасности; Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать	методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;
Уметь	выполнять работы по оптимизации схем управления автоматизированной системой; - применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;
Владеть	навыками определения возможных векторов атаки на автоматизированную систему; и осуществлять выбор средств защиты информации

6. Структура и содержание практики/НИР

Общая трудоемкость практики/НИР составляет 15 зачетных единиц 540 акад. часов, в том числе:
– контактная работа – 10,1 акад. часов:
– самостоятельная работа – 529,9 акад. часов;
– форма промежуточной аттестации – зачет с оценкой

№ 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 исследованиz подготовка литературного обзора	10	Реферат, статья по заданной теме, доклад на студенческой научной конференции университета	ПСК-7.1, ОПК-5, ПК-1, ПК-2, ПК-6, ПК-7, ПК-16, ПК-24
2.	Проведение научно-исследовательской работы	10	Промежуточный отчет о выполнении НИР	ПСК-7.1, ОПК-5, ПК-1, ПК-2, ПК-6, ПК-7, ПК-16, ПК-24
3.	Составление отчета о научно-исследовательской работе	10	Отчет о научно-исследовательской работе	ПСК-7.1, ОПК-5, ПК-1, ПК-2, ПК-6, ПК-7, ПК-16, ПК-24
4.	Защита выполненной работы	10	Заключение кафедры об уровне исследования	ПСК-7.1, ОПК-5, ПК-1, ПК-2, ПК-6, ПК-7, ПК-16, ПК-24

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. http://znanium.com/bookread2.php?book=957144

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
2. УнижаевН.В. Информационно-аналитическое обеспечение безопасности орга-низации: учебное пособие/Унижаев Н.В.–СПб.: Издательскийцентр «Интермедия», 2018.–408с. https://ibooks.ru/reading.php?productid=356934
3. Обеспечение безопасности персональных данных при их обработке в информацион-ных системах персональных данных: Учебное пособие / Е.Г. Воробьев –СПб.: Изда-тельский центр «Интермедия», 2016. –432 с. https://ibooks.ru/reading.php?productid=351534
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
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
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
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.
8. Шаньгин, В.Ф Комплексная защита информации в корпоративных системах [Элек-тронный 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.
9. Баранкова, И. И. 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). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1031-7. - Сведения доступны также на CD-ROM.

10. Баранкова, И. И. Разработка БД в MS SQL Server с использованием SSMS : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3473.pdf&show=dcatalogues/1/1514290/3473.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1207-6. - Сведения доступны также на CD-ROM.
11. Баранкова, И. И. Разработка приложений на C# для работы с базами данных : практикум / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3748.pdf&show=dcatalogues/1/1527762/3748.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
12. Баранкова, И. И. Теория информации. Кодирование : учебное пособие / И. И. Баранкова, М. В. Коновалов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3313.pdf&show=dcatalogues/1/1137756/3313.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1073-7. - Сведения доступны также на CD-ROM.
13. Баранкова, И. И. 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). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
14. Демиденко, Л. Л. 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. - ISBN 978-5-9967-1653-1. - Загл. с титул. экрана. - URL : https://magtu.informsystema.ru/uploader/fileUpload?name=3964.pdf&show=dcatalogues/1/1532465/3964.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.
15. Калугина, О. Б. Объектно-ориентированное программирование : учебное пособие / О. Б. Калугина, М. В. Надеина, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2015. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=1286.pdf&show=dcatalogues/1/1123483/1286.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст :

электронный. - Сведения доступны также на CD-ROM.

16. Калугина, О. Б. Практикум по теории графов : практикум / О. Б. Калугина, Т. Н. Носова, Г. И. Лукьянова ; МГТУ. - Магнитогорск : МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3444.pdf&show=dcatalogues/1/1514250/3444.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

17. Королева, В. В. Практикум по математической статистике : практикум / 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://magtu.informsystema.ru/uploader/fileUpload?name=3967.pdf&show=dcatalogues/1/1532478/3967.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

18. Носова, Т. Н. Создание классов в C#: интерактивный справочно-обучающий практикум : практикум / Т. Н. Носова ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3807.zip&show=dcatalogues/1/1529974/3807.zip&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

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). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - ISBN 978-5-9967-1305-9. - Текст : электронный. - Сведения доступны также на CD-ROM.

20. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; 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://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

21. Теория графов и ее приложения : учебное пособие / О. Б. Калугина, В. В. Баранкова, Т. Н. Носова, Г. И. Лукьянов ; МГТУ. - Магнитиогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3371.pdf&show=dcatalogues/1/1139223/3371.pdf&view=true (дата обращения: 14.05.2020). - Макрообъект. - Текст : электронный. - ISBN 978-5-9967-1078-2. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:
Методические указания по выполнению самостоятельных работ по производственной-практике (Приложение 2) .

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows 7	Д-757-17 от 27.06.2017	27.07.2018
MS Office 2007	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View	https://dlib.eastview.com/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение	URL: http://www1.fips.ru/
Национальная информационно-аналитическая	URL:
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers
Электронные ресурсы библиотеки МГТУ им. Г.И.	http://magtu.ru:8085/marcweb
Федеральный образовательный портал – Экономика.	http://ecsocman.hse.ru/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и	http://webofscience.com
Международная реферативная и полнотекстовая	http://scopus.com
Международная база полнотекстовых журналов	http://link.springer.com/
Международная коллекция научных протоколов по	http://www.springerprotocols.
Международная база научных материалов в области	http://materials.springer.com/
Международная база справочных изданий по всем	http://www.springer.com/refer
Международная реферативная и полнотекстовая	https://www.nature.com/sitein
Архив научных журналов «Национальный	https://archive.neicon.ru/xmlu
Банк данных угроз безопасности информации	https://bdu.fstec.ru/

9 Материально-техническое обеспечение 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-3M.

Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»

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»

ПРИЛОЖЕНИЕ 1

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».

Оценка «отлично» выставляется обучающемуся, выполнившему задание на проведение НИР в полном объеме, исчерпывающе, грамотно и логически стройно излагающему основные результаты работы. При этом обучающийся не затрудняется с ответами на задаваемые ему вопросы в ходе защиты отчета по НИР, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами решения практических задач.

Оценка «хорошо» выставляется обучающемуся выполнившему задание на проведение НИР в полном объеме, грамотно и по существу излагающего его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми приемами их решения.

Оценка «удовлетворительно» выставляется обучающемуся выполнившему задание на проведение НИР в полном объеме, но допускает неточности, недостаточно правильные формулировки, нарушения последовательности в изложении программного материала и испытывает трудности в выполнении практических заданий.

Оценка «неудовлетворительно» выставляется обучающемуся, который не выполнил задание на проведение НИР.

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 инраструктуры
- Принципы построения модели надежности системы управления кибербезопасностью АСУ ТП

ПРИЛОЖЕНИЕ 2

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.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.