МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

ПРОГРАММА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	10

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Программа научно-исследовательской работы составлена:
зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент:
зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1 Цели научно-исследовательской работы

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 научно-исследовательской работы

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 научно-исследовательской работы в структуре образовательной программы

В соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 10.05.03 «Информационная безопасность автоматизированных систем», научно-исследовательская работа относится к разделу «Практики». При выполнении научно-исследовательской работы обучающиеся опираются на знания, умения и навыки, полученные в ходе предшествующего изучения дисциплин базовой и вариативной части. Выполнение научно-исследовательской работы необходимо для подготовки выпускной квалификационной работы.

4 Место проведения научно-исследовательской работы

Научно-исследовательская работа проводится на базе кафедры информатики и информационной безопасности.

5 Компетенции обучающегося, формируемые в результате выполнения научно-исследовательской работы и планируемые результаты

В результате выполнения научно-исследовательской работы у обучающего должны быть сформированы следующие компетенции:

Структурный элемент компетенции	Планируемые результаты обучения
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. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации. Подходы 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

Структурный элемент компетенции	Планируемые результаты обучения
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 -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 -применять специализированные 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	-основами построения моделей систем передачи информации -навыками пользования библиотеками прикладных программ для решения прикладных задач -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

Структурный элемент компетенции	Планируемые результаты обучения
	-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 (ПК-16)	
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;

Структурный элемент компетенции	Планируемые результаты обучения
	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; выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;
Владеть	навыками определения возможных векторов атаки на автоматизированную систему;
ПСК-7.1 – способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	− цели и задачи моделирования систем и процессов защиты информации; этапы моделирования и виды моделей систем и процессов защиты информации;- способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - различные информационные технологии, используемые в моделировании процессов 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	- приемами исследования проблем моделирования процессов защиты информации, возникающих в различных сферах человеческой деятельности - 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

6 Структура и содержание научно-исследовательской работы

Общая трудоемкость научно-исследовательской работы 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	Этап выполнения НИР	Семестр	Вид работы	Код и структурный элемент компетенции
1	планирование научно-исследовательской работы, включающее ознакомление с тематикой исследовательских работ в области информационной безопасности, выбор темы исследовани подготовка литературного обзора	А	Реферат, статья по заданной теме, доклад на студенческой научной конференции университета	ОПК-5 зув; ПК-1 зув; ПК-2 зув; ПК-6 зув; ПК-7 зув; ПК-16 зув; ПК-24 зув; ПСК-7.1 зув
2	проведение научно-исследовательской работы	А	Промежуточный отчет о выполнении НИР	ОПК-5 зув; ПК-1 зув; ПК-2 зув; ПК-6 зув; ПК-7 зув; ПК-16 зув; ПК-24 зув; ПСК-7.1 зув
3	составление отчета о научно-исследовательской работе	А	Отчет о научно-исследовательской работе	ОПК-5 зув; ПК-1 зув; ПК-2 зув; ПК-6 зув; ПК-7 зув; ПК-16 зув; ПК-24 зув; ПСК-7.1 зув
4	защита выполненной работы	А	Заключение кафедры об уровне исследования	ОПК-5 зув; ПК-1 зув; ПК-2 зув; ПК-6 зув; ПК-7 зув; ПК-16 зув; ПК-24 зув; ПСК-7.1 зув

Рабочие задания составляются преподавателями профилирующих дисциплин для каждого обучающегося индивидуально, учитывая особенности предприятия

7 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?

7 Учебно-методическое и информационное обеспечение научно-исследовательской работы

а) Основная литература:

1) 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. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true . - Макрообъект. - ISBN 978-5-9967-1031-7.
4. 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
5. 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
6. 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
7. 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
8. 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.
9. 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.

Интернет – ресурсы

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" http://www.studentlibrary.ru/catalogue/switch_kit/x2016-034.html
2. Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: https://bdu.fstec.ru .– Загл. с экрана. Яз. рус.
3. 1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
4. 2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_18.htm – Загл. с экрана. Яз. рус.
5. 3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
6. 4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".http://www.osp.ru/os/– Загл. с экрана. Яз. рус.
7. 5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.
8. 6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru . Яз. рус.
9. 7. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

10. 8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
11. 9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/ .– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение научно-исследовательской работы

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - - выход в Интернет.
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплект учебного оборудования «Беспроводные компьютерные сети ЭВМ»; Комплект учебного оборудования «Системы контроля доступа»; Комплект учебного оборудования «Сенсорные сети ZigBee в системах автоматического управления»; Комплект учебного оборудования «Сетевая безопасность» SECURITY-CISCO-3M; Модуль «Низкоуровневый контроллер Ethernet».
Лаборатория систем передачи информации, ауд. 2124	Стенд коммуникационного оборудования с сервером для моделирования облачного сервиса.
Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine - Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office 2007 (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - Выход в Интернет и с доступ в электронную информационно-образовательную среду университета