

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

П ВГУ 2.1.02.100501С – 2016

УТВЕРЖДАЮ

Первый проректор-
проректор по учебной работе


_____ Е.Е. Чупандина

«30» 12 2016 г

ПОЛОЖЕНИЕ

о порядке проведения практик обучающихся
в Воронежском государственном университете
по специальности
10.05.01 Компьютерная безопасность

Специализация «Анализ безопасности компьютерных систем»
Специалитет

РАЗРАБОТАНО – рабочей группой факультета компьютерных наук

ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ – декан факультета компьютерных наук
Э.К. Алгаинов

ИСПОЛНИТЕЛЬ – доцент кафедры технологий обработки и защиты информации
В.В. Гаршина

ВВЕДЕНО В ДЕЙСТВИЕ приказом ректора 30.12.2016 № 1118

ВВОДИТСЯ ВЗАМЕН П ВГУ 2.1.02.100501С – 2016

СРОК ПЕРЕСМОТРА при изменении ФГОС

1 Область применения

Настоящее Положение обязательно для обучающихся по направлению подготовки 10.05.01 Компьютерная безопасность (специализация «Анализ безопасности компьютерных систем») и научно-педагогических работников Воронежского государственного университета (далее – Университета) обеспечивающих подготовку по направлению по указанной основной образовательной программе.

2 Нормативные ссылки

Настоящее Положение разработано в соответствии со следующими нормативными документами:

ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1512;

Приказ Министерства образования и науки Российской Федерации от 12 сентября 2013 года N 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования»;

И ВГУ 2.1.12 – 2015 Инструкция о порядке проведения практик обучающихся в Воронежском государственном университете по основным образовательным программам высшего образования.

3 Общие положения

3.1 Виды практик, типы и способы проведения

В соответствии с ФГОС ВО по специальности Компьютерная безопасность в практическую подготовку студентов входят следующие виды практик: учебная и производственная, в том числе преддипломная практики, а также научно-исследовательская работа.

Типы учебной практики:

- учебная ознакомительная;
- учебно-лабораторный практикум;
- учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности;
- учебная экспериментально-исследовательская практика;
- учебный сбор (Военный блок).

По способу проведения учебные практики являются стационарными.

По форме проведения все типы учебных практик являются концентрированными, за исключением учебно-лабораторного практикума, форма проведения которого является рассредоточенной.

Типы производственной практики:

- производственная практика по получению профессиональных умений и опыта профессиональной деятельности;
- производственная конструкторская практика;
- производственная технологическая и эксплуатационная практика;
- производственная преддипломная практика;
- войсковая стажировка (Военный блок).

По способу проведения производственные практики являются стационарными.

По форме проведения все типы производственных практик являются концентрированными,

Производственная практика завершается проведением итоговой конференции по результатам производственной практики. На конференции студенты отчитываются по итогам прохождения практики, сдают всю необходимую документацию. По итогам конференции групповой руководитель от факультета с учетом мнения руководителей от предприятий (форма отзыва руководителя от предприятия приведена в Приложении А) выставляет оценку по производственной практике каждому обучающемуся.

Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной.

Производственные практики проводятся в индивидуальном порядке, учебные – в составе учебных подгрупп.

Проведение научно-исследовательской работы осуществляется в индивидуальном порядке. Каждому студенту назначается научный руководитель, который определяет тему научно-исследовательской работы, разрабатывает план работ и контролирует процесс выполнения.

Все виды и типы практик соответствуют видам деятельности, на которые направлена основная образовательная программа по специальности 10.05.01 Компьютерная безопасность: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная.

3.2 Общие требования к организации практик (по видам практик)

Согласно п. 6.7 ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, практика является составной частью профессиональной образовательной программы и представляет собой одну из форм организации учебного процесса, заключающуюся в профессионально-практической подготовке обучающихся на базах практик. Перечень, объем и виды практик определяются Ученым советом факультета компьютерных наук Университета с учетом требований ФГОС и фиксируются учебным планом. Основные требования к практикам определяются ФГОС ВО по специальности Компьютерная безопасность и настоящим Положением.

Учебная ознакомительная практика является первым звеном в цикле учебных практик в системе профессионального образования специалистов, обучающихся по специальности 10.05.01 Компьютерная безопасность специализация «Анализ безопасности компьютерных систем». Она соответствует виду деятельности - организационно-управленческая, научно-исследовательская. Этот вид учебной практики ориентирован на ознакомление студентов с организационной структурой, принципами функционирования, информационными технологиями и политикой информационной безопасности применяемыми в локальных сетях Университета, функционированием автоматизированной информационной системы (АИС) ВГУ, системой управления электронным документооборотом вуза. Задачами ознакомительной учебной практики является освоение современных информационных технологий, применяемых в научных исследованиях, специального программного обеспечения и оборудования для задач анализа защищенности объектов информатизации, а также получение практического опыта работы с подсистемой информационного обеспечения и электронного документооборота автоматизированной информационной системы (АИС) ВГУ.

Учебно-лабораторный практикум закрепляет знания студентов о современных численных методах алгебры, математического анализа и обыкновенных дифференциальных уравнений, полученных в ходе изучения дисциплины «Методы вычислений», которая входит в базовую часть учебного плана основной

образовательной программы. Он соответствует одному из видов деятельности, на которые направлена основная образовательная программа – проектная деятельность. Этот практикум ориентирован на то, чтобы расширить знания студентов о методике алгоритмизации, тестирования и исследования в вычислительном эксперименте методов алгебры, математического анализа и обыкновенных дифференциальных уравнений; научить студентов применять полученные знания при решении прикладных задач; способствовать получению фундаментальных знаний в ходе самостоятельной исследовательской работы; способствовать дальнейшему развитию системного и логического мышления.

Учебная практика по получению первичных профессиональных умений и навыков является следующим звеном в цикле учебных практик. Она соответствует одному из видов деятельности, на которые направлена основная образовательная программа - научно-исследовательская деятельность. Эта практика ориентирована: на получение первичных профессиональных умений и навыков в области: работы с научной литературой; участия в научно-исследовательских проектах в соответствии с профилем объекта профессиональной деятельности; изучение защищаемых компьютерных систем и входящих в них средств обработки, хранения и передачи информации; изучение систем управления информационной безопасностью компьютерных систем; изучение методов и реализующие их средств защиты информации в компьютерных системах; изучение математических моделей процессов, возникающих при защите информации, обрабатываемой в компьютерных системах; применение методов и реализующие их систем и средств контроля эффективности защиты информации в информационных системах; составления научных обзоров, рефератов и библиографии по тематике проводимых исследований; участия в работе научных семинаров, научно-тематических конференций; подготовки научных и научно-технических публикаций.

Учебная экспериментально-исследовательская практика является заключительным звеном в цикле учебных практик. Она ориентирована на два вида деятельности: научно-исследовательскую и контрольно-аналитическую. Учебная экспериментально-исследовательская практика направлена на изучение студентами современных информационных технологий, применяемых в научных исследованиях и производственных задачах, специального программного обеспечения и оборудования для задач анализа защищенности объектов информатизации. В ходе прохождения практики обучающиеся изучают: методики работы с измерительной аппаратурой для контроля и анализа отдельных характеристик процессов, приборов, устройств; программного обеспечения информационных систем для решения задач обеспечения информационной безопасности; знакомятся с методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации; приобретают опыт самостоятельного решения учебной технологической задачи, исследований и экспериментов, а также практическим применением современных информационных технологий.

Учебная практика проводится на базе структурных подразделений Университета, научно-исследовательских институтов, аналитических центров в составе Университета.

Важным элементом практической подготовки студентов является научно-исследовательская работа студентов. Основной ее задачей является приобретение опыта в исследовании актуальной научной проблемы, углубление и закрепление теоретических знаний, полученных студентами при изучении обще-профессиональных и спе-

циальных дисциплин, а также развитие у студентов интереса к научно-исследовательской работе, привитие им навыков проведения научных исследований.

Основные результаты и фактические материалы, полученные в период прохождения учебной практики и выполнения научно-исследовательской работы, могут быть использованы студентом при выполнении итоговой квалификационной работы, а также при подготовке докладов и сообщений на студенческих научно-практических конференциях.

Неотъемлемой частью процесса профессионального образования специалистов, обучающихся по направлению Информационная безопасность, является серия производственных практик. Производственная практика организуется для обеспечения непосредственной связи обучения с производством и ознакомления обучающихся с одним из возможных направлений будущей профессиональной деятельности.

Первым звеном в цикле производственных практик является производственная практика по получению профессиональных умений и опыта профессиональной деятельности. Она ориентирована на вид деятельности - научно-исследовательская. Целями ее проведения являются: расширение теоретической подготовки, полученной в вузе, практическими знаниями; приобретение опыта проведения самостоятельного исследования и решения практической научной задачи. В процессе прохождения практики решается ряд задач: знакомство студентов с современными информационными технологиями в области информационной защиты, применяемых на профильных предприятиях (организациях); получение обучающимися навыков самостоятельного проведения экспериментальных исследований, подбора, изучения и обобщения научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности.

Следующим типом производственной практики является – производственно-конструкторская практика. Она соответствует двум видам деятельности – проектная и организационно-управленческая. Целями ее проведения являются: расширение теоретической подготовки, полученной в вузе, практическими знаниями; приобретение опыта самостоятельного решения практической проектной задачи. В процессе прохождения практики решается ряд задач: формирование у студентов умений и навыков проведения технологического обследования объекта информационной защиты; сбора экспериментального и экспертного материала и его теоретического обобщения; разработки технических предложений. Проводится ознакомление студентов с применяемой в профильной организации измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач информационной безопасности. Обучающиеся приобретают опыт самостоятельного решения проектной задачи, проведения экспериментальных исследований, а также проведение предварительного технико-экономического обоснования проектных расчетов, навыки разработки технологической и эксплуатационной документации.

Следующим типом производственной практики является – производственная технологическая и эксплуатационная практика. Она ориентирована на три вида деятельности – эксплуатационную, проектную, организационно-управленческую. Данный тип практики направлен на приобретение практических навыков и компетенций в сфере профессиональной деятельности по обеспечению информационной безопасности, а также приобщение специалистов к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций. Во время прохождения практики студенты получают знания по организации и управлению деятельностью подразделения, где проводится практика правила эксплуатации и особенности применяемого оборудования; стандарты, положения и инструкции по деятельности подраз-

деления; принципы формирования комплекса мер по обеспечению информационной безопасности предприятия. Получают опыт работы с технологическим или измерительным оборудованием, проведения мониторинга угроз информационной безопасности; оценку соответствия выполненной работы техническому заданию и действующим нормативным документам.

Завершающим звеном в цепи производственных практик является - производственная преддипломная практика. Ее целью является проведение систематизации, расширения, закрепление и углубления теоретических профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки, а также формирование у студентов навыков ведения самостоятельной научной работы, исследования и экспериментирования. Основные результаты и фактические материалы, полученные в период прохождения производственной преддипломной практики, могут быть использованы студентом при выполнении итоговой квалификационной работы, а также при подготовке докладов и сообщений на студенческих научно-практических конференциях.

Базами производственной практики могут выступать:

- научные и ведомственные организации, связанные с решением научных и технических задач;
- научно-исследовательские и вычислительные центры;
- научно-производственные объединения;
- образовательные организации среднего профессионального и высшего образования;
- органы государственной власти;
- организации, осуществляющие разработку и использование информационных систем, научных достижений, продуктов и сервисов в области информационных технологий.

Практика, как правило, осуществляется на основе договоров о прохождении производственной практики или двухсторонних соглашений между Университетом и предприятиями, учреждениями, организациями, независимо от их организационно-правовых форм и форм собственности, в соответствии с которыми указанные предприятия, учреждения и организации предоставляют места для прохождения практики.

С целью ежегодного успешного проведения практики руководители практики от факультета систематически обновляют и дополняют базу данных организаций, принимающих студентов для прохождения практики.

Обучающиеся могут самостоятельно осуществлять поиск мест практики. При выборе мест прохождения практики студенты руководствуются рекомендациями руководителя практики от факультета. Базовые предприятия для студентов должны соответствовать профилю подготовки специалиста, располагать квалифицированными кадрами для руководства практикой студента и - иметь материально-техническую и ИКТ базу с инновационными технологиями.

От учреждения или предприятия, выбранного в качестве места прохождения производственной практики, студент обязан предоставить договор, подтверждающий готовность данной организации обеспечить студенту возможность прохождения практики. Перед прохождением практики студент должен получить в деканате направление на практику и сдать его на предприятие, принимающее его на производственную практику.

Базы производственной преддипломной практики определяются индивидуальными руководителями практики (руководителями выпускных

квалификационных работ). Заключение договоров с базами этой практики не предусмотрено. В качестве баз производственной преддипломной практики выступают: научные и ведомственные организации, связанные с решением научных и технических задач; научно-исследовательские и вычислительные центры; научно-производственные объединения; образовательные организации среднего профессионального и высшего образования; органы государственной власти; организации, осуществляющие разработку и использование информационных систем, научных достижений, продуктов и сервисов в области IT-технологий. Базой производственной преддипломной практики могут выступать также структурные подразделения Университета.

Учебная и производственная практика, предусмотренная по военному блоку, проводятся Военным учебным центром Университета по установленным Военным центром программам. Содержание программ данных практик включает компоненты, содержащие гостайну. Результаты прохождения практик хранятся также в Военном учебном центре Университета.

4 Программы практик

Учебная ознакомительная практика

Цели учебной ознакомительной практики

Целью учебной ознакомительной практики является ознакомление студентов со спецификой получаемой специальности, с объектами будущей работы, подготовка студентов к осознанному и углубленному изучению обще-профессиональных и специальных дисциплин для последующего освоения общих и профессиональных компетенций по направлению специализированной подготовки в области защиты информации.

Задачи учебной ознакомительной практики

Задачами учебной исследовательской практики являются:

- ознакомление с функционированием локальных сетей в условиях университета, функционированием автоматизированной информационной системы (АИС) ВГУ, системой управления электронным документооборотом вуза;
- ознакомление с технологиями информационной защиты, применяемых в автоматизированной информационной системе (АИС) ВГУ и на рабочих местах пользователей;
- ознакомление с современными информационными технологиями, применяемыми в научных исследованиях, специального программного обеспечения и оборудования для задач анализа защищенности объектов информатизации;
- получение практического опыта работы с подсистемой информационного обеспечения и электронного документооборота автоматизированной информационной системы (АИС) ВГУ.

Время проведения учебной ознакомительной практики

2 курс, 4 семестр.

Содержание учебной ознакомительной практики

Общая трудоемкость практики составляет 2 зачетные единицы, 72 учебных часа.

Разделы (этапы) практики:

подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ;

учебный ознакомительный этап: ознакомление с работой (АИС) ВГУ, применяемыми в ней технологиями защиты информации и изучение рекомендуемой литературы; проведение обзора современных информационных технологий, специального про-

граммного обеспечения, оборудования, для решения задач анализа защищенности объекта информатизации; проведение самостоятельного решения учебной задачи, исследований и экспериментов;

этап - оформление отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Научно-исследовательские и научно-производственные технологии, используемые на учебной практике. При прохождении учебной практики работа студента подразумевает практическое использование средств вычислительной техники, современных информационных технологий, применяемых в научных исследованиях, специального программного обеспечения и оборудования для задач анализа защищенности объекта информатизации, а также изучение различных информационных технологий, стандартов в области информационной безопасности объектов и систем, функционирование локальных сетей в условиях университета, функционирование автоматизированной информационной системы (АИС) Университета.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

- способность 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);

- способность к самоорганизации и самообразованию (ОК-8).

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 1. Перечень фонда оценочных средств учебной ознакомительной практики

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики. Приложение Г.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL: http://biblioclub.ru/index.php?page=book&id=112247 >
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с.<URL: http://www.methodolog.ru/books/mni.pdf >

3	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
4	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил. — (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
5	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

б) дополнительная литература:

№ п/п	Источник
6	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. — Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
7	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. — 2010.— Вып. 20. — № 2. — 350 с.
8	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
9	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
10	<i>Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.</i>
11	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. — Воронеж: Воронежский институт МВД России, 2014. — 186 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
12	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
13	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
14	Портал государственных услуг Российской Федерации www.gosuslugi.ru
15	http://www.cryptopro.ru
16	http://www.infotecs.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя. Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов приведен в ФОС (Приложение Г).

Контрольные вопросы – типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения учебной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. Представленный отчет по практике оценивается на соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы учебной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения учебной ознакомительной практики в рамках самостоятельной работы на месте прохождения практики, при выполнении различных видов работ под руководством руководителя практики от кафедры (Табл. 2).

Таблица 2. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-5 способность 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	Знать - цели, задачи, принципы и основные направления обеспечения информационной безопасности; - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства;	Этап - учебный ознакомительный	ФОС: Отчет по практике. Собеседование по вопросам Приложение Г.
	Уметь - пользоваться современной научнотехнической информацией по исследуемым проблемам и задачам.		ФОС: Собеседование по тексту отчета по практике.

	Владеть Методами обработки и анализа научно-технической информацией по исследуемым проблемам и задачам.		ФОС: Собеседование, анализ выполнения практического задания.
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам.	Этапы: - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: Собеседование по тексту отчета по практике
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации.		ФОС: выполненное в ходе прохождения практики задание
	Владеть - методиками саморазвития, самостоятельного приобретения и освоения новых знаний - навыками критической оценки своих достоинств и недостатков - опытом выбора средств и возможностей развития достоинств и устранения недостатков		ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 2. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количества баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Материально-техническое обеспечение (для практик, проводимых в Университете)

Лаборатория аппаратных средств вычислительной техники (корп.1, ауд. № 213). Состав лаборатории аппаратных средств вычислительной техники: Компьютеры Intel Core i3 4160 (3600), Intel Celeron D341, Лабораторный стенд «Архитектура ЭВМ».

Лаборатория программно-аппаратных средств обеспечения информационной безопасности (корп. 1б, ауд. № 303п). Состав лаборатории программно-аппаратных средств обеспечения информационной безопасности: персональные компьютеры на базе Intel Atom-330 1.6 ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-

считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528.

Лаборатория технической защиты информации (корп. 1а, ауд. № 384а). Состав лаборатории технической защиты информации: ST033P "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИПЗ, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель (5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>.

Лаборатория безопасности компьютерных сетей (корп. 1 ауд. 384) Состав лаборатории безопасности компьютерных сетей: рабочие места - персональные компьютеры HP-3500-PRO на базе Intel i3-2120, мониторы ЖК 22" (16 шт.), стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, версии 7.0 для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

Порядок представления отчетности по практике

Для аттестации студент предъявляет задание руководителя на прохождение практики и оформляет результаты практики в виде отчета. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях Б, В.

Учебно-лабораторный практикум

Цели учебно-лабораторного практикума

Закрепить знания студентов о современных численных методах алгебры, математического анализа и обыкновенных дифференциальных уравнений, а также способах их исследования в вычислительном эксперименте применительно к анализу и синтезу моделируемых систем.

Задачи учебно-лабораторного практикума

Задачами учебно-лабораторного практикума являются:

- закрепить знания студентов в области численных методов алгебры, математического анализа, обыкновенных дифференциальных уравнений, научить применять полученные знания при решении прикладных задач;
- расширить знания студентов о методике алгоритмизации, тестирования и исследования в вычислительном эксперименте методов алгебры, математического анализа и обыкновенных дифференциальных уравнений;
- способствовать получению фундаментальных знаний в ходе самостоятельной исследовательской работы;
- способствовать дальнейшему развитию системного и логического мышления.

Время проведения учебно-лабораторного практикума

3 курс, 5, 6 семестр.

Формы проведения: рассредоточенная.

Содержание учебно-лабораторного практикума

Общая трудоемкость учебной ознакомительной практики составляет 2 зачетные единицы, 74 часа.

Разделы (этапы) практики:

подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ;

учебно-исследовательский этап: определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор специального программного обеспечения и инструментальных средств для решения поставленной задачи;

практический лабораторный этап: проведение самостоятельного решения учебной прикладной задачи, выполнение тестирования и исследования в вычислительном эксперименте численных методов алгебры, математического анализа и обыкновенных дифференциальных уравнений;

этап оформления отчёта по итогам практики: описание проделанной работы с самооценкой результатов учебно-лабораторного практикума; формулирование выводов и предложений по организации практикума;

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

– способность к самоорганизации и самообразованию (ОК-8).

Обще-профессиональные компетенции (ОПК):

– способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

– способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

Формы промежуточной аттестации (по итогам учебно-лабораторного практикума)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по учебно-лабораторному практикуму

Таблица 3. Перечень фонда оценочных средств учебно-лабораторного практикума

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практикума. Приложение Д.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения учебно-лабораторного практикума ”
2	Практическое задание	Соответствует заданию на практикум. Приложение Е.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения учебно-лабораторного практикума ”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Демидович Б. П. Основы вычислительной математики : учеб. пособие / Б. П. Демидович, И. А. Марон. — Москва : Лань, 2011. — 664 с. Режим доступа: https://lanbook.lib.vsu.ru/books/element.php?pl1_cid=25&pl1_id=2025
2	Демидович Б. П. Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения : учеб. пособие / Б. П. Демидович, И. А. Марон, Э. З. Шувалова. — Москва : Лань, 2010. — 400 с. Режим доступа: https://lanbook.lib.vsu.ru/books/element.php?pl1_cid=25&pl1_id=537
3	Амосов А. А. Вычислительные методы / А. А. Амосов, Ю. А. Дубинский, Н. В. Копченова. — Москва : Лань, 2014. — 672 с. Режим доступа: https://lanbook.lib.vsu.ru/books/element.php?pl1_cid=25&pl1_id=42190

б) дополнительная литература:

№ п/п	Источник
4	Бахвалов Н. С. Численные методы : учеб. пособие для студ. физ.-мат. специальностей вузов / Н. С. Бахвалов, Н. П. Жидков, Г. М. Кобельков. — Москва : БИНОМ. Лаб. знаний, 2007. — 636 с.
5	Калиткин Н. Н. Численные методы : учеб. пособие для студ. вузов / Н. Н. Калиткин ; под ред. А. А. Самарского. — Москва : Наука, 1978. — 512 с.
6	Турчак Л. И. Основы численных методов : учеб. пособие для студ. вузов / Л. И. Турчак, П. В. Плотников. — Москва : Физматлит, 2005. — 300 с.
7	Самарский А. А. Введение в численные методы : учеб. пособие для вузов / А. А. Самарский. — Санкт-Петербург : Лань, 2005. — 288 с.
8	Самарский А. А. Численные методы : учеб. пособие для студ. вузов / А. А. Самарский, А. В. Гулин. — Москва : Наука : Физматлит, 1989. — 429 с.
9	Самарский А. А. Задачи и упражнения по численным методам : учеб. пособие / А. А. Самарский, П. Н. Вабищевич, Е. А. Самарская. — Москва : Эдиториал УРСС, 2000. — 207 с.
10	Бахвалов Н. С. Численные методы в задачах и упражнениях : учеб. пособие / Н. С. Бахвалов, А. В. Лапин, Е. В. Чижонков ; под ред. В. А. Садовниченко. — Москва : Высш. шк., 2000. — 189 с.
11	Пирумов У. Г. Численные методы : учеб. пособие для студ. вузов / У. Г. Пирумов. — Москва : Дрофа, 2004. — 221 с.
12	Численные методы : сборник задач : учеб. пособие для студ. вузов / В. Ю. Гидаспов [и др.] ; под ред. У. Г. Пирумова. — Москва : Дрофа, 2007. — 144 с.
13	Гудович Н. Н. Избранные вопросы курса численных методов. Вып. 1 : Интерполяция алгебраическими многочленами. Многочлен Лагранжа / Н. Н. Гудович. — Воронеж, 2002. — 36 с.
14	Гудович Н. Н. Избранные вопросы курса численных методов. Вып. 2 : Многочлен Ньютона / Н. Н. Гудович. — Воронеж, 2002. — 28 с.
15	Гудович Н. Н. Избранные вопросы курса численных методов. Вып. 3 : Интерполяция кубическими сплайнами / Н. Н. Гудович. — Воронеж, 2002. — 35 с.
16	Гудович Н. Н. Избранные вопросы курса численных методов. Вып. 4 : Численное интегрирование / Н. Н. Гудович. — Воронеж, 2002. — 36 с.
17	Гудович А. Н. Избранные вопросы курса численных методов. Вып. 6 : Сеточные приближения производных / А. Н. Гудович, Н. Н. Гудович. — Воронеж, 2006. — 31 с.

18	Гудович А. Н. Избранные вопросы курса численных методов. Вып. 7 : Одношаговые методы решения задачи Коши / А. Н. Гудович, Н. Н. Гудович. — Воронеж, 2006. — 31 с.
19	Гудович Н. Н. Избранные вопросы курса численных методов. Вып. 10 : Сеточные методы для уравнений в частных производных / Н. Н. Гудович. — Воронеж, 2007. — 34 с.
20	Численное решение задачи Коши для обыкновенных дифференциальных уравнений методами типа Рунге-Кутта : метод. указания по курсу «Численные методы». Ч. 1 / сост. В. В. Корзунина, З. А. Шабунина. — Воронеж, 2002. — 53 с.
21	Численное решение задачи Коши для обыкновенных дифференциальных уравнений методами типа Рунге-Кутта : метод. указания по курсу «Численные методы». Ч. 2 : Индивидуальные задания / сост. В. В. Корзунина, З. А. Шабунина. — Воронеж, 2005. — 31 с.
22	Метод дифференциальной прогонки решения краевых задач для обыкновенных дифференциальных уравнений : учеб.-метод. пособие / сост. В. В. Корзунина, З. А. Шабунина, Д. В. Шаруда. — Воронеж : ЛОП ВГУ, 2006. — 27 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
23	www.lib.vsu.ru — Зональная научная библиотека ВГУ
24	Волков Е. А. Численные методы : учеб. пособие / Е. А. Волков. — Москва : Лань, 2008. — 256 с. Режим доступа: https://lanbook.lib.vsu.ru/books/element.php?pl1_cid=25&pl1_id=54
25	Корзунина В. В. Лабораторный практикум по численным методам : учеб. пособие. Ч. 1 : Теория / В. В. Корзунина, З. А. Шабунина. — Воронеж : ИПЦ ВГУ, 2011. Режим доступа: http://www.lib.vsu.ru/elib/texts/method/vsu/m11-139.pdf
26	Корзунина В. В. Лабораторный практикум по численным методам : учеб. пособие. Ч. 2 : Индивидуальные задания / В. В. Корзунина, З. А. Шабунина. — Воронеж : ИПЦ ВГУ, 2011. Режим доступа: http://www.lib.vsu.ru/elib/texts/method/vsu/m11-140.pdf
27	Корзунина В. В. Лабораторный практикум по численным методам : уравнения математической физики : метод. пособие для вузов / В. В. Корзунина, З. А. Шабунина, Д. В. Шаруда. — Воронеж : ЛОП ВГУ, 2006. — 22 с. Режим доступа: http://www.lib.vsu.ru/elib/texts/method/vsu/may07053.pdf
28	Лабораторные занятия по численным методам: интерполирование и приближение функций : учеб.-метод. пособие. Ч. 1 : Теория / В. В. Корзунина, К. П. Лазарев, З. А. Шабунина. — Воронеж : Издательский дом ВГУ, 2014. — 32 с. Режим доступа: http://www.lib.vsu.ru/elib/texts/method/vsu/m14-92.pdf
29	Лабораторные занятия по численным методам: интерполирование и приближение функций : учеб.-метод. пособие. Ч. 2 : Индивидуальные задания / В. В. Корзунина, К. П. Лазарев, З. А. Шабунина. — Воронеж : Издательский дом ВГУ, 2014. — 19 с. Режим доступа: http://www.lib.vsu.ru/elib/texts/method/vsu/m14-93.pdf

Критерии оценивания результатов практики

Оценка по учебно-лабораторному практикуму выставляется руководителем практикума от кафедры на основе содержания отчета студента. Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечни контрольных вопросов и практических заданий приведены в ФОС (Приложениях Д и Е).

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период проведения практикума.

Отчет по практикуму должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. Представленный отчет по практикуму оценивается на соответствие информации и данным из материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы учебно-лабораторного практикума являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практикума в рамках самостоятельной работы студентов (Табл. 4).

Таблица 4. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы работы и анализа научно-технической информации по исследуемым проблемам и задачам.	Этапы: – учебно-исследовательский, - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	Отчет по практике. ФОС: Собеседование по вопросам Приложение Г.
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации.		ФОС: Собеседование по тексту отчета по практике.
	Владеть - методиками саморазвития, самостоятельно приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков.		ФОС: Собеседование, анализ выполнения практического задания.

ОПК-2 способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать - численные методы алгебры, математического анализа, обыкновенных дифференциальных уравнений; - методы анализа и синтеза моделируемых систем; - математические методы обработки экспериментальных данных.	Этапы: - практический лабораторный; - оформления отчёта по итогам практики; - устный доклад по результатам самостоятельной работы.	ФОС: Собеседование по тексту отчета по практике.
	Уметь - применять полученные знания при решении прикладных задач численных методов; - строить математические модели задач профессиональной области.		ФОС: выполненное в ходе прохождения практики задание.
	Владеть - методами количественного анализа процессов обработки, поиска и передачи информации; - навыками использования математического аппарата в экспериментальных исследованиях.		ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.
ОПК-8 способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач	Знать - стандартные программные средства и методики алгоритмизации, тестирования и исследования в вычислительном эксперименте.	Этапы: - практический лабораторный; - оформления отчёта по итогам практики; - устный доклад по результатам самостоятельной работы	ФОС: Собеседование по тексту отчета по практике
	Уметь - применять полученные знания для проведения исследования в вычислительном эксперименте при решении прикладных задач численных методов.		ФОС: выполненное в ходе прохождения практики задание.
	Владеть - навыками применения стандартных программных средств при выполнении тестирования и исследования в вычис-		ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета

	лительном эксперименте; - навыками использования известных методов программирования и возможностей базового языка программирования для решения типовых профессиональных задач.		по практике.
--	---	--	--------------

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практикума являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 4. Формирование этих дескрипторов происходит в течение всего периода практикума, в рамках выполнения самостоятельной работы.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количества баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует

оценке - «хорошо»;

- выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

- требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Материально-техническое обеспечение (для практик, проводимых в Университете)

Лабораторный класс с проектором (корп.1, ауд. № 12). Состав лаборатории: ПК AMD Phenom II X4 (10 шт.), ПК Intel Celeron (3 шт.), мультимедиа-проектор Acer x1273, коммутатор D-Link DES-1016D.

Лабораторный класс с проектором (корп.1, ауд. № 20). Состав лаборатории: коммутатор HP ProCurve 1400-24G, мультимедиа-проектор Acer x1161, ПК Intel Core i3 4160 (3600) (14 шт.), ПК AMD Phenom II X4 (10 шт.), ПК AMD Athlon 64 X2 (1 шт.)

Лабораторный класс с проектором (корп.1, ауд. № 216). Состав лаборатории: коммутатор D-Link DES-1016D, мультимедиа-проектор Optoma EP723, ПК Intel Core i3 4160 (3600) (15 шт.)

Мультимедийная аудитория (корп.1, ауд. № 433). Состав аудитории: ПК Intel Pentium DualCore, мультимедиа-проектор Optoma EP780.

Порядок представления отчетности по практикуму

Для аттестации студент оформляет результаты практикума в виде отчета. Требования к оформлению отчета представлены в Приложениях Б, В.

Учебная практика

по получению первичных профессиональных умений и навыков

Цели учебной практики по получению первичных профессиональных умений и навыков

Целью учебной практики является формирование первичных профессиональных умений и навыков исследования и формализации прикладных задач по защите информации.

Задачи учебной практики по получению первичных профессиональных умений и навыков

Задачами учебной практики по получению первичных профессиональных умений и навыков являются:

- получение студентами первичных сведений по обеспечению комплексной защиты информации в различных типах организаций, знакомство с правовым регулированием обеспечения информационной безопасности;

- знакомство со специальным программным обеспечением и оборудованием для решения поставленной задачи по анализу защищенности объекта информатизации;

- получение студентами опыта исследования и анализа поставленной учебной задачи, составлению обзора и обоснование выбора современных информационных технологий, необходимых для решения задачи;

- проведение самостоятельного решения учебной научной задачи, исследований и экспериментов;

- составление итогового отчета по результатам разработки, исследования и формализации поставленной учебной задачи.

Время проведения учебной практики по получению первичных профессиональных умений и навыков

5 курс, 9 семестр.

Содержание учебной практики по получению первичных профессиональных умений и навыков

Общая трудоемкость практики составляет 3 зачетные единицы, 108 учебных часов.

Разделы (этапы) практики:

подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ;

учебно-исследовательский этап: определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий, применяемых в научных исследованиях специального программного обеспечения и оборудования, для решения поставленной задачи по анализу защищенности объекта информатизации; проведение самостоятельного решения учебной научной задачи, исследований и экспериментов;

этап оформления отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Выполняемые на практике учебные задания могут быть разделены на несколько групп, в том числе:

– научно-исследовательские, цель которых – создание новых методов решения поставленных в ходе практики задач, в том числе математического или компьютерного инструментария для их исследования;

– прикладные, целью которых является постановка и решение конкретных задач методами, изученными в ходе освоения дисциплин ОП;

– обзорно-аналитические, целью которых является изучение и сравнительный анализ различных методов решения возникающих на практике задач с последующими рекомендациями по их применению.

Научно-исследовательские и научно-производственные технологии, используемые в учебной практике. В процессе прохождения учебной практики работа студента подразумевает: практическое использование средств вычислительной техники; современных информационных технологий, применяемых в научных исследованиях; специального программного обеспечения и оборудования для задач анализа защищенности объекта информатизации; изучение различных информационных технологий и стандартов в области информационной безопасности объектов и систем; функционирование локальных сетей в условиях университета; функционирование автоматизированной информационной системы (АИС) Университета.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

– способность к самоорганизации и самообразованию (ОК-8).

Обще-профессиональные компетенции (ОПК):

– способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки ин-

формации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

– способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4).

Профессиональные компетенции (ПК):

– способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1).

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 5. Перечень фонда оценочных средств учебной практики по получению первичных профессиональных умений и навыков

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики. Приложение Ж.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. <URL:http://www.methodolog.ru/books/mni.pdf>
3	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
4	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил. — (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
5	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см. — (Админи-

	стрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122 >.
--	---

б) дополнительная литература:

№ п/п	Источник
6	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
7	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
8	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Сборник законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
9	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Сборник законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
10	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
11	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
12	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
13	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
14	Портал государственных услуг Российской Федерации www.gosuslugi.ru
15	http://www.cryptopro.ru
16	http://www.infotecs.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя и выступления студента с презентацией по результатам практики. Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов приведен в ФОС (Приложение Ж).

Контрольные вопросы – типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения учебной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок.

ческих ошибок. Представленный отчет по практике оценивается на соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы учебной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения учебной ознакомительной практики в рамках самостоятельной работы на месте прохождения практики, при выполнении различных видов работ под руководством руководителя практики от кафедры (Табл. 6).

Таблица 6. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам.	Этапы: - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики	ФОС: Собеседование по тексту отчета по практике
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации.		ФОС: выполненное в ходе прохождения практики задание.
	Владеть - методиками саморазвития, самостоятельного приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения		ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике/

<p>ОПК-3 способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации</p>	<p>недостатков.</p> <p>Знать</p> <ul style="list-style-type: none"> - основные понятия информатики; - назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных. <p>Уметь</p> <ul style="list-style-type: none"> - использовать расчетные формулы, таблицы, графики, компьютерные программы для решения прикладных математических задач. <p>Владеть</p> <ul style="list-style-type: none"> - навыками поиска информации в сети Интернет, работы с офисными приложениями, работы с СУБД; - навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач. 	<p>Этапы:</p> <ul style="list-style-type: none"> - учебно-исследовательский, - оформления отчёта по итогам практики. 	<p>ФОС: Собеседование по тексту отчета.</p> <p>ФОС: Собеседование на защите отчета по практике.</p>
<p>ОПК-4 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p>	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обобщения, восприятия и анализа информации; - методы анализа причинно-следственных связей; - основные естественнонаучные законы, применение математического аппарата для решения профессиональных задач; - методы программирования и методы разработки эффективных алгоритмов решения прикладных задач. <p>Уметь</p>	<p>Этап - учебно-исследовательский этап.</p>	<p>ФОС: Собеседование по тексту отчета.</p> <p>текст отчета, доклад</p>

	<ul style="list-style-type: none"> - выявлять сущность проблем, возникающих в ходе профессиональной деятельности; - формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области. 		и презентация по результатам самостоятельной работы по теме практики.
	<p>Владеть</p> <ul style="list-style-type: none"> - профессиональной терминологией; - навыками применения современных методов научных исследований; - пользоваться современной научнотехнической информацией по исследуемым проблемам и задачам. 		
ПК-1 способность осуществлять подбор, изучение и обобщение научнотехнической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	<p>Знать</p> <ul style="list-style-type: none"> - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации 	<p>Этапы:</p> <ul style="list-style-type: none"> - учебно-исследовательский, - выполнение самостоятельных работ по теме практики, - оформления отчёта. 	ФОС: Практическое задание, текст доклада и презентация по результатам самостоятельной работы по теме практики.
	<p>Уметь</p> <ul style="list-style-type: none"> - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации. 		ФОС: Собеседование на защите отчета по практике.
	<p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовыми актами по тех- 		ФОС: Ответы на вопросы на защите отчета по практике Отзыв руководителя практики.

	нической защите информации.		
--	-----------------------------	--	--

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 6. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык)

не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Материально-техническое обеспечение (для практик, проводимых в Университете)

Лаборатория аппаратных средств вычислительной техники (корп.1, ауд. № 213). Состав лаборатории аппаратных средств вычислительной техники: Компьютеры Intel Core i3 4160 (3600), Intel Celeron D341, Лабораторный стенд «Архитектура ЭВМ».

Лаборатория программно-аппаратных средств обеспечения информационной безопасности (корп. 1б, ауд. № 303п). Состав лаборатории программно-аппаратных средств обеспечения информационной безопасности: персональные компьютеры на базе Intel Atom-330 1.6 ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528.

Лаборатория технической защиты информации (корп. 1а, ауд. № 384а). Состав лаборатории технической защиты информации: ST033P "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИПЗ, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель (5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>.

Лаборатория безопасности компьютерных сетей (корп. 1 ауд. 384) Состав лаборатории безопасности компьютерных сетей: рабочие места - персональные компьютеры HP-3500-PRO на базе Intel i3-2120, мониторы ЖК 22" (16 шт.), стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, версии 7.0 для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

Порядок представления отчетности по практике

Для аттестации студент предъявляется заданию руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях Б, В.

Учебная экспериментально-исследовательская практика

Цели учебной экспериментально-исследовательской практики

Целью учебной экспериментально-исследовательской практики является развитие профессиональных знаний и компетенций студентов на базе учебных задач, для решения которых необходимо использовать современные информационные технологии обработки и защиты информации.

Задачи учебной экспериментально-исследовательской практики

Задачами учебной экспериментально-исследовательской практики являются:

- знакомство с современными информационными технологиями, применяемыми в научных исследованиях и производственных задачах, специальным программным обеспечением и оборудованием для задач анализа защищенности объектов информатизации;
- освоение методик работы с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности;
- знакомство с методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации;
- приобретение опыта самостоятельного решения учебной задачи, исследований и экспериментов, а также практическим применением современных информационных технологий;
- составление итогового отчета по результатам разработки, исследования и формализации поставленной учебной задачи.

Время проведения учебной экспериментально-исследовательской практики
6 курс, В семестр.

Содержание учебной экспериментально-исследовательской практики

Общая трудоемкость практики составляет 3 зачетные единицы, 108 учебных часов.

Разделы (этапы) практики:

подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ;

учебно-исследовательский этап: определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий, специального программного обеспечения и оборудования, для решения поставленной задачи по анализу защищенности объекта информатизации;

научно-экспериментальный этап: проведение самостоятельного решения учебной задачи, работа с измерительной аппаратурой, выполнение типовых расчетов и моделирование процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации;

этап оформления отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики;

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Научно-исследовательские и научно-производственные технологии, используемые на учебной практике. При прохождении учебной практики работа студента подразумевает практическое использование средств вычислительной техники, современных информационных технологий, применяемых в научных исследованиях, специального программного обеспечения и оборудования для задач анализа защищенности объекта информатизации, а также изучение различных информационных технологий, стандартов в области информационной безопасности объектов и систем, функционирование локальных сетей в условиях университета, функционирование автоматизированной информационной системы (АИС) Университета.

Результаты освоения, коды формируемых (сформированных) компетенций
Общекультурные компетенции (ОК):

- способность к самоорганизации и самообразованию (ОК-8).

Обще-профессиональные компетенции (ОПК):

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4).

Профессиональные компетенции (ПК):

- способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2);

- способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы (ПК-9);

- способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации (ПК-11).

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 7. Перечень фонда оценочных средств учебной экспериментально-исследовательской практики

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики. Приложение 3.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. — М.: Либроком. 2010 – 280 с. <URL:http://www.methodolog.ru/books/mni.pdf>
3	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.

4	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : MapT, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
5	Фостер, Джеймс. Защита от взлома: сокет, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>
6	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
7	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
8	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
9	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

б) дополнительная литература:

№ п/п	Источник
10	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
11	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
12	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
13	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
14	<i>Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Курсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.</i>
15	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
16	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа:

	http://smwww.main.vsu.ru
17	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
18	Портал государственных услуг Российской Федерации www.gosuslugi.ru
19	http://www.cryptopro.ru
20	http://www.infotecs.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента. Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов приведен в ФОС (Приложение 3).

Контрольные вопросы – типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения учебной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. Представленный отчет по практике оценивается на соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы учебной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения учебной экспериментально-исследовательской практики в рамках самостоятельной работы на месте прохождения практики, при выполнении различных видов работ под руководством руководителя практики от кафедры (Табл. 8).

Таблица 8. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам.	Этапы: - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: Собеседование по тексту отчета по практике.
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им;		ФОС: выполненное в ходе прохождения практики задание.

	<ul style="list-style-type: none"> - пользоваться современными источниками научно-технической информации. 		
	<p>Владеть</p> <ul style="list-style-type: none"> - методиками саморазвития, самостоятельного приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков. 		<p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>
ОПК-4 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обобщения, восприятия и анализа информации; - методы анализа причинно-следственных связей; - основные естественнонаучные законы, применение математического аппарата для решения профессиональных задач; - методы программирования и методы разработки эффективных алгоритмов решения прикладных задач. <p>Уметь</p> <ul style="list-style-type: none"> - выявлять сущность проблем, возникающих в ходе профессиональной деятельности; - формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области. 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - научно-экспериментальный. 	<p>ФОС: Собеседование по тексту отчета по практике.</p>
	<p>Владеть</p> <ul style="list-style-type: none"> - профессиональной терминологией; - навыками применения современных методов научных исследований; - пользоваться современной научно-технической информацией по исследуемым проблемам и зада- 	<p>Этап - оформление отчёта по итогам практики.</p>	<p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике.</p>

	чам.		
ПК-2 способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - методы и средства контроля эффективности технической защиты информации; - основные методы управления информационной безопасностью.	Этап - научно-экспериментальный.	ФОС: Собеседование, анализ выполнения практического задания.
	Уметь - оценивать информационные риски в информационных системах; - работать с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем.		
	Владеть - методами управления информационной безопасностью информационных систем; - методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации; - методами оценки информационных рисков.		
ПК-9 способность участвовать в проведении	Знать - основы организационного и правового обеспече-	Этап - научно-экспериментальный.	ФОС: Собеседование на защите отчета по практи-

экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	<p>ния информационной безопасности;</p> <ul style="list-style-type: none"> - основные нормативные правовые акты в области информационной безопасности и защиты информации. 		ке, вопросы Приложение 3.
	<p>Уметь</p> <ul style="list-style-type: none"> - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации. 	<p>Этапы:</p> <ul style="list-style-type: none"> - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики. 	<p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>
	<p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовыми актами по технической защите информации. 		
ПК-11 способность участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	<p>Знать</p> <ul style="list-style-type: none"> - технические каналы утечки информации; - возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам; - методы и средства контроля эффективности технической защиты информации. 		ФОС: Собеседование на защите отчета по практике, вопросы Приложение 3.
	<p>Уметь</p> <ul style="list-style-type: none"> - анализировать и оценивать угрозы информационной безопасности объектов; - проводить мониторинг угроз безопасности информационных систем; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для оценки защищенности компьютерных систем. 		ФОС: анализ отчета по выполнению практического задания на практике.
	<p>Владеть</p> <ul style="list-style-type: none"> - методами и средствами выявления угроз безопасности; 		

	- методами формирования требований по защите информации.		
--	--	--	--

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 8. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык)

не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Материально-техническое обеспечение (для практик, проводимых в Университете)

Лаборатория аппаратных средств вычислительной техники (корп.1, ауд. № 213). Состав лаборатории аппаратных средств вычислительной техники: Компьютеры Intel Core i3 4160 (3600), Intel Celeron D341, Лабораторный стенд «Архитектура ЭВМ».

Лаборатория программно-аппаратных средств обеспечения информационной безопасности (корп. 1б, ауд. № 303п). Состав лаборатории программно-аппаратных средств обеспечения информационной безопасности: персональные компьютеры на базе Intel Atom-330 1.6 ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528.

Лаборатория технической защиты информации (корп. 1а, ауд. № 384а). Состав лаборатории технической защиты информации: ST033P "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИПЗ, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель (5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>.

Лаборатория безопасности компьютерных сетей (корп. 1 ауд. 384) Состав лаборатории безопасности компьютерных сетей: рабочие места - персональные компьютеры HP-3500-PRO на базе Intel i3-2120, мониторы ЖК 22" (16 шт.), стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, версии 7.0 для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

Порядок представления отчетности по практике

Для аттестации студент предъявляется заданию руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях Б, В.

Научно-исследовательская работа (НИР)

Цели научно-исследовательской работы

Целями научно-исследовательской работы являются:

- подготовка студента к решению задач, относящихся к различным проблемам комплексного обеспечения информационной безопасности, а также к решению отдельных фундаментальных проблем, связанных с компьютерной безопасностью;
- углубление и закрепление теоретических знаний, полученных студентами при изучении общепрофессиональных и специальных дисциплин;

- приобретение и совершенствование студентами профессиональных навыков и умений, закрепляющих полученные теоретические знания;
- развитие у студентов интереса к научно-исследовательской работе, привитие им навыков проведения исследований;
- проведение исследований, непосредственно связанных с выпускной квалификационной работой (ВКР).

Задачи научно-исследовательской работы

Основной задачей научно-исследовательской работы является приобретение опыта в исследовании актуальной научной проблемы, а также подбор необходимых материалов для выполнения выпускной квалификационной работы.

Во время научно-исследовательской практики студент должен:

изучить:

- информационные источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;
- методы моделирования и исследования вопросов информационной безопасности;
- методы анализа и обработки данных, являющихся входными для проведения научного исследования;
- информационные технологии, применяемые в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;
- требования к оформлению научно-технической документации;

выполнить:

- анализ, систематизацию и обобщение информации по теме исследований;
- сравнение результатов исследования объекта разработки с отечественными и зарубежными аналогами;
- анализ научной и практической значимости проводимых исследований.

Время проведения:

5 курс, А семестр.

Форма проведения: рассредоточенная.

Содержание научно-исследовательской работы: общая трудоемкость производственной преддипломной практики составляет 2 зачетные единицы, 72 часа.

Разделы (этапы) НИР.

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ.

Выбор направления исследований: выбор темы исследования; определение проблемы, объекта и предмета исследования; формулирование цели и задач исследования; теоретический анализ литературы и исследований по проблеме, подбор необходимых источников по теме (патентные материалы, научные отчеты, техническая документация и др.); составление библиографии; формулирование рабочей гипотезы.

Выполнение теоретических и экспериментальных исследований: проведение обзора и выбор современных информационных технологий, разработка специального математического, алгоритмического и программного обеспечения, выбор оборудования для решения поставленной задачи по анализу защищенности объекта информатизации; проведение самостоятельного решения научной задачи, исследований и экспериментов.

Обобщение и оценка результатов исследований, составление отчетной документации: описание проделанной работы с самооценкой результатов выполнения НИР; формулирование выводов и предложений по организации НИР.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

- способность к самоорганизации и самообразованию (ОК-8);
- Общепрофессиональные компетенции (ОПК):
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);
- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

Профессиональные компетенции (ПК):

- способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1);
- способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2);

Форма промежуточной аттестации (по итогам выполнения НИР):

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по НИР

Таблица 9. Перечень фонда оценочных средств научно-исследовательской работы

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Доклад, сообщение	Примерные темы НИР. Приложение И, К.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате выполнения НИР”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1.	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2.	Новиков А.М., Новиков Д.А. Методология научного исследования. — М.: Либроком. 2010 — 280 с.<URL:http://www.methodolog.ru/books/mni.pdf>
3.	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] — 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014. — 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
4.	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : MapT, 2008 .— 287

	с. : ил. — (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
5.	Ищевнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищевнов, М.В. Мещатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
6.	Фостер, Джеймс. Защита от взлома: сокет, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
7.	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
8.	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
9.	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
10.	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
11.	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.
12.	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

б) дополнительная литература:

№ п/п	Источник
13.	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
14.	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
15.	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 — Загл. с экрана.
16.	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
17.	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации

	Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
18.	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
19.	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
20.	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
21.	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
22.	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
23.	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
24.	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
25.	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
26.	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
27.	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
28.	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
29.	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
30.	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII междунар. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
31.	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
32.	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное об-

	разование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
33.	Андрианов В.И. "Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
34.	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
35.	Брусницин Н.А. Открытость и шпионаж / Н.А.Брусницин. – М.: Воениздат, 1991.
36.	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
37.	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
38.	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
39.	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
40.	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
41.	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
42.	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
43.	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
44.	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный. - Загл. с экрана.
45.	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. : ил. — Библиогр.: с.95 .— <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf >
46.	Портал государственных услуг Российской Федерации www.gosuslugi.ru
47.	http://www.cryptopro.ru
48.	http://www.infotecs.ru
49.	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows.Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич,ООО "ЛИССИ". Источник: RSDN Magazine #3-2006
50.	http://www.lissi-crypto.ru/
51.	http://www.signal-com.ru
52.	http://www.shipka.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем НИР на основе содержания отчета студента, выступления с презентацией и ответов на вопросы на конференции по итогам НИР. Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень вопросов и заданий приведен в ФОС (Приложение И, К).

Контрольные вопросы и задания - типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на выполнение НИР.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период выполнения НИР.

Отчет по НИР должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы производственной преддипломной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практики в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя НИР (Табл.10).

Таблица 10. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	Форма отчетности по НИР, ФОС* (средства оценивания)
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам.	Этапы – выполнение теоретических и экспериментальных исследований, - обобщение и оценка результатов исследований, - составление отчетной документации.	ФОС: Собеседование на защите отчета по НИР.
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации.		ФОС: Собеседование на защите отчета по НИР.
	Владеть - методиками саморазвития, самостоя-		ФОС: Текст доклада и презентация по результатам

	<p>тельного приобретения и освоения новых знаний;</p> <ul style="list-style-type: none"> - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков. 		НИР. Собеседование на защите отчета по НИР.
ОПК-3 способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	<p>Знать</p> <ul style="list-style-type: none"> - определение информации и ее роль в развитии общества. 	<p>Этапы:</p> <ul style="list-style-type: none"> - выбор направления исследований, - выполнение теоретических и экспериментальных исследований, - обобщение и оценка результатов исследований, - составление отчетной документации 	ФОС: Собеседование на защите отчета по НИР.
	<p>Уметь</p> <ul style="list-style-type: none"> - применять современные информационные технологии для поиска и обработки информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации. 		ФОС: Собеседование на защите отчета по НИР.
	<p>Владеть</p> <ul style="list-style-type: none"> - навыками поиска и автоматизированной обработки информации. 		ФОС: Текст доклада и презентация по результатам НИР. Отзыв руководителя НИР.
ОПК-4 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обобщения, восприятия и анализа информации; - методы анализа причинно-следственных связей; - основные естественнонаучные законы, применение математического аппарата для решения профессиональных задач; - методы програм- 	<p>Этапы:</p> <ul style="list-style-type: none"> - выполнение теоретических и экспериментальных исследований, - обобщение и оценка результатов исследований, - составление отчетной документации. 	ФОС: Собеседование на защите отчета по НИР.

	мирования и методы разработки эффективных алгоритмов решения прикладных задач.		
	<p>Уметь</p> <ul style="list-style-type: none"> - выявлять сущность проблем, возникающих в ходе профессиональной деятельности; - формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области. 		<p>ФОС: Собеседование на защите отчета по НИР.</p>
	<p>Владеть</p> <ul style="list-style-type: none"> - профессиональной терминологией; - навыками применения современных методов научных исследований; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. 		<p>ФОС: Ответы на вопросы на защите отчета по НИР Отзыв руководителя НИР.</p>
<p>ПК-1</p> <p>способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности</p>	<p>Знать</p> <ul style="list-style-type: none"> - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации. 	<p>Этапы:</p> <ul style="list-style-type: none"> - выбор направления исследований; - выполнение теоретических и экспериментальных исследований; - обобщение и оценка результатов исследований, - составление отчетной документации. 	<p>ФОС: Собеседование на защите отчета по НИР.</p>
	<p>Уметь</p> <ul style="list-style-type: none"> - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации. 		<p>ФОС: Собеседование на защите отчета по НИР.</p>

	<p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовыми актами по технической защите информации. 		<p>ФОС: Ответы на вопросы на защите отчета по НИР Отзыв руководителя НИР.</p>
<p>ПК-2</p> <p>способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований</p>	<p>Знать</p> <ul style="list-style-type: none"> - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - методы и средства контроля эффективности технической защиты информации; - основные методы управления информационной безопасностью. 	<p>Этапы:</p> <ul style="list-style-type: none"> - выполнение теоретических и экспериментальных исследований; - обобщение и оценка результатов исследований, - составление отчетной документации. 	<p>ФОС: Собеседование по тексту отчета по НИР.</p>
	<p>Уметь</p> <ul style="list-style-type: none"> - оценивать информационные риски в информационных системах; - работать с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных си- 		<p>ФОС: текст доклада и презентация по результатам самостоятельной работы по НИР.</p>

	стем. Владеть - методами управления информационной безопасностью информационных систем; - методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации; - методами оценки информационных рисков.		ФОС: текст доклада и презентация по результатам работы по НИР.
--	--	--	--

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате выполнения НИР

Конечными результатами освоения программы НИР являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 10. Формирование этих дескрипторов происходит в течение всего периода выполнения НИР, в рамках выполнения самостоятельной работы выполнении различных видов работ под руководством руководителя НИР.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие от-

вета, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Порядок представления отчетности по НИР

Для аттестации студент предьявляется заданием руководителя на выполнение НИР и оформляет результаты в виде отчета и готовит выступление с презентацией по результатам выполнения НИР. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложении Б, В.

Производственная практика по получению профессиональных умений и опыта профессиональной деятельности

Цели производственной практики по получению профессиональных умений и опыта профессиональной деятельности

Целями производственной практики по получению профессиональных умений и опыта профессиональной деятельности являются: закрепление и углубление теоретической подготовки, получение опыта производственной работы; приобретение практических навыков и компетенций в сфере профессиональной деятельности по использованию программного обеспечения; технологий и средств обеспечения безопасности информационных систем, а также приобщение студентов к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций.

Задачи производственной практики по получению профессиональных умений и опыта профессиональной деятельности

– знакомство с деятельностью профильной организации, специальным программным обеспечением и оборудованием;

– получение студентом опыта исследования и освоения современных информационных технологий в области информационной защиты;

– получение опыта использования математических методов и компьютерных технологий в области научно-исследовательской деятельности в условиях производства;

– приобретение опыта самостоятельного проведения экспериментальных исследований;

- выработка у студентов навыков работы с технологической и эксплуатационной документацией;

- приобретение опыта взаимодействий с представителями организации, презентации результатов технических предложений, подготовки и оформления документации.

Время проведения производственной практики по получению профессиональных умений и опыта профессиональной деятельности

6 курс, В семестр.

Содержание производственной практики по получению профессиональных умений и опыта профессиональной деятельности

Общая трудоемкость производственной конструкторской практики составляет 3 зачетные единицы, 108 часов.

Разделы (этапы) практики:

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ, ознакомление студентов с организационной структурой профильной организации, применяемой аппаратурой и программным обеспечением.

Научно-исследовательский этап: знакомство с деятельностью профильной организации, специальным программным обеспечением и оборудованием определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий.

Производственный этап: сбор экспериментального и экспертного материала и его теоретическое обобщение; проведение самостоятельного решения учебной задачи, исследований и экспериментов; разработка технических предложений.

Оформление отчёта по итогам практики: описание проделанной работы с учетом действующих нормативных и методических документов; формулирование выводов и предложений по организации практики.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

- способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

- способность к самоорганизации и самообразованию (ОК-8).

Обще-профессиональные компетенции (ОПК):

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4).

Профессиональные компетенции (ПК):

- способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1).

Формы промежуточной аттестации (по итогам практики)

зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 11. Перечень фонда оценочных средств по производственной практике по получению профессиональных умений и опыта профессиональной деятельности

№ п/п	Наименование оценочного	Представление оценочного средства в фонде	Критерии оценки
-------	-------------------------	---	-----------------

	средства		
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики, Приложение Ж,З	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с.<URL:http://www.methodolog.ru/books/mni.pdf>
3	Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. - М. : Академия, 2007. – 330 с.
4	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
5	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6	Олейник П. П. Корпоративные информационные системы: для бакалавров и специалистов: учебник для студ. вузов, обуч. по направл. 080800 "Прикладная информатика (по областям)" и др. экон. спец. – СПб. : Питер, 2012. – 176 с.
7	Фостер, Джеймс. Защита от взлома: сокеты, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 р. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
9	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
10	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виера ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viera .— ISBN 5-9706-0027-X .—

	<URL: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118 >.
11	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
12	Проскурин В. Г. Защита программ и данных - М. : Академия, 2011. – 198 с.
13	Управление внедрением информационных систем: курс лекций: учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. технологий / В.И. Грекул, Г. Н. Денищенко, Н.Л. Коровкина. – М.: Интернет-Ун-т информ. технологий, 2008. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/2196/267/info/ .
14	Юрин И.Ю. Теоретические и практические основы защиты информации. 2012. http://library.sgu.ru/uch_lit/620.pdf

б) дополнительная литература:

№ п/п	Источник
14	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
15	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
16	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 — Загл. с экрана.
17	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
18	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
19	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
20	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
21	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
22	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
23	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
24	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
25	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государ-

	ственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
26	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
27	Ермошкин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. М. : Изд-во Московского гуманитарного университета, 2003.
28	Корнеев И.К., Степанов Е.А. Защита информации в офисе. – "Издательство Проспект", 2008. – 333 с.
29	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
30	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
31	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII междунаrod. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
32	Партыка Т.Л. Информационная безопасность М.: ФОРУМ, 2007
33	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
34	Андрианов В.И. "Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
35	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
37	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
38	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
39	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
40	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
41	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
42	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
43	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
44	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
45	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный. - Загл. с экрана.
46	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголевых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. :

	ил. — Библиогр.: с.95 .— <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf >
47	Портал государственных услуг Российской Федерации www.gosuslugi.ru
48	http://www.cryptopro.ru
49	http://www.infotecs.ru
50	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows.Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич,ООО “ЛИССИ”. Источник: RSDN Magazine #3-2006
51	http://www.lissi-crypto.ru/
52	http://www.signal-com.ru
53	http://www.shipka.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы на конференции по итогам практики.

Проводится собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов и примерных вариантов заданий приведен в ФОС (Приложение Ж, 3).

Контрольные вопросы и задания - типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения производственной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы производственной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», описанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практики в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя (Табл.12).

Таблица 12. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-6 способность работать в коллективе, толерантно воспринимая социальные, культурные и иные разли-	Знать - принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов.	Этапы: – подготовительный, - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: Отзыв руководителя практики.

чия	<p>Уметь</p> <ul style="list-style-type: none"> - работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия. 	<p>Этапы:</p> <ul style="list-style-type: none"> - подготовительный, - научно-исследовательский, - производственный. 	<p>ФОС: Отзыв руководителя практики.</p>
	<p>Владеть</p> <ul style="list-style-type: none"> - навыками общения с коллегами при решении производственных задач. 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - производственный 	<p>ФОС: Отзыв руководителя практики.</p>
ОК-8 способность к самоорганизации и самообразованию	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обработки и анализа научнотехнической информации по исследуемым проблемам и задачам. 	<p>Этапы:</p> <ul style="list-style-type: none"> - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики. 	<p>ФОС: собеседование по тексту отчета по практике.</p>
	<p>Уметь</p> <ul style="list-style-type: none"> - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научнотехнической информации. 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - производственный, - доклад по результатам самостоятельной работы по теме практики. 	<p>ФОС: выполненное в ходе прохождения практики задание.</p>
	<p>Владеть</p> <ul style="list-style-type: none"> - методиками саморазвития, самостоятельного приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков. 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - производственный 	<p>ФОС: текст доклада и презентация по результатам самостоятельной работы на практике, собеседование на защите отчета по практике.</p>
ОПК-4 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и ин-	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обобщения, восприятия и анализа информации; - методы анализа причинно-следственных связей; - основные естественнонаучные законы, применение математического аппарата для решения профессио- 	<p>Этап:</p> <ul style="list-style-type: none"> - научно-исследовательский, - выполнение самостоятельных работ по теме практики, - доклад. 	<p>ФОС: Ответы на вопросы на защите отчета по практике. Отзыв руководителя практики.</p>

новационными проектами	нальных задач; - методы программирования и методы разработки эффективных алгоритмов решения прикладных задач.		
	Уметь - выявлять сущность проблем, возникающих в ходе профессиональной деятельности; - формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области.	Этапы: - научно-исследовательский, - производственный, - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: текст доклада и презентация по результатам самостоятельной работы на практике, собеседование на защите отчета по практике.
	Владеть - профессиональной терминологией; - навыками применения современных методов научных исследований; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.	Этапы: - подготовительный, - научно-исследовательский, - производственный, - доклад по результатам работы по теме практики.	ФОС: собеседование, анализ выполнения практического задания.
ПК-1 способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации.	Этапы: - учебно-исследовательский, - выполнение самостоятельных работ по теме практики, - оформления отчёта.	ФОС: Практическое задание, текст доклада и презентация по результатам самостоятельной работы по теме практики.
	Уметь - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации.	Этапы: - подготовительный, - научно-исследовательский, - оформление отчета, - доклад о результатах работы по теме практики.	ФОС: Собеседование на защите отчета по практике.
	Владеть - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовыми актами по технической защите информации.	Этапы: - подготовительный, - научно-исследовательский, - оформление отчета, - доклад о результатах работы по теме практики.	ФОС: Ответы на вопросы на защите отчета по практике. Отзыв руководителя практики.

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 12. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Порядок представления отчетности по практике

Для аттестации студент предъявляется дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит

выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях А, Б, В.

Производственная конструкторская практика

Цели производственной конструкторской практики

Целью производственной конструкторской практики является получение профессиональных умений и навыков исследования и формализации прикладных задач в проектной форме, а также поэтапной разработки проекта по организации информационной защиты.

Задачи производственной конструкторской практики

Задачами производственной конструкторской практики являются:

- знакомство со специальным программным обеспечением и оборудованием для решения поставленной производственной проектной задачи;
- получение студентом опыта исследования и анализа задачи, составлению обзора и обоснования выбора современных информационных технологий необходимых для решения задачи;
- проведение самостоятельного решения производственной проектной задачи, исследований и экспериментов;
- составления промежуточного и итогового отчетов по результатам разработки, оформление документации к проекту по действующим правилам и стандартам.

Время проведения производственной конструкторской практики

6 курс, В семестр.

Содержание производственной конструкторской практики

Общая трудоемкость производственной конструкторской практики составляет 3 зачетные единицы, 108 часов.

Разделы (этапы) практики:

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ, ознакомление студентов с организационной структурой профильной организации, применяемой аппаратурой и программным обеспечением.

Проектно-конструкторский этап: определение проектной задачи для разработки технологических решений в проектной форме; проведение технологического обследования объекта информационной защиты: сбор экспериментального и экспертного материала и его теоретическое обобщение; проведение самостоятельного решения производственной задачи, исследований и экспериментов; разработка технических предложений.

Оформление отчёта по итогам практики: описание проделанной работы с учетом действующих нормативных и методических документов; формулирование выводов и предложений по организации практики.

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Научно-исследовательские и научно-производственные технологии, используемые на производственной конструкторской практике. При прохождении производственной конструкторской практики работа студента подразумевает практическое использование средств вычислительной техники, специального программного обеспечения и оборудования для анализа защищенности объекта информатизации, а также изучение различных информационных технологий, стандартов в области информационной безопасности объектов и систем.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

- способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
 - способность к самоорганизации и самообразованию (ОК-8).
- Профессиональные компетенции (ПК):
- способность способностью участвовать в разработке проектной и технической документации (ПК-6);
 - способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7);
 - способность участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8).
 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-15).

Формы промежуточной аттестации (по итогам практики)

зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 13. Перечень фонда оценочных средств по производственной конструкторской практике

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики, Приложение И.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с.<URL:http://www.methodolog.ru/books/mni.pdf>
3	Митрофанова Е.Ю., Сирота А.А. Методические указания по оформлению выпускных работ бакалавров / Е.Ю., Митрофанова, А.А. Сирота, учебно-методическое пособие, - Воронеж: Издательский дом ВГУ, 2016 – 23 с.
4	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.

5	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил. — (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мещатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
7	Фостер, Джеймс. Защита от взлома: сокет, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
9	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
10	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
11	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
12	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.
13	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

б) дополнительная литература:

№ п/п	Источник
14	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
15	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
16	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 — Загл. с экрана.

17	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. — 2010.— Вып. 20. — № 2. — 350 с.
18	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
19	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
20	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
21	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
22	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
23	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
24	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
25	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
26	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
27	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
28	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
29	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
30	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
31	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII междунаод. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
32	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.

33	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
34	Андреанов В.И. "Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
35	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
36	Брусницын Н.А. Открытость и шпионаж / Н.А.Брусницын. – М.: Воениздат, 1991.
37	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
38	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
39	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
40	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
41	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
42	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
43	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
44	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
45	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный. - Загл. с экрана.
46	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. : ил. — Библиогр.: с.95 .— <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf >
47	Портал государственных услуг Российской Федерации www.gosuslugi.ru
48	http://www.cryptopro.ru
49	http://www.infotecs.ru
50	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows.Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич,ООО "ЛИССИ". Источник: RSDN Magazine #3-2006
51	http://www.lissi-crypto.ru/
52	http://www.signal-com.ru
53	http://www.shipka.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы на конференции по итогам практики.

Проводятся собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов и примерных вариантов заданий приведен в ФОС (Приложение И).

Контрольные вопросы и задания - типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения производственной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы производственной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практики в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры (Табл.14).

Таблица 14. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-6 способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знать - научные основы, цели, принципы, методы и технологии управленческой деятельности; -- принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов	Этапы: - подготовительный, - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: Отзыв руководителя практики.
	Уметь - работать в коллективе, принимать управленческие решения и оценивать их эффективность; - работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодей-	Этапы: - подготовительный, - проектно-конструкторский	ФОС: Отзыв руководителя практики.

	ствия в коллективе, толерантно воспринимать эти различия.		
	Владеть - навыками общения с коллегами при решении производственных задач.	Этап – проектно-конструкторский	ФОС: Отзыв руководителя практики.
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научнотехнической информации по исследуемым проблемам и задачам.	Этапы: - оформления отчёта по итогам практики, - устный доклад по результатам самостоятельной работы по теме практики.	ФОС: Собеседование по тексту отчета по практике.
	Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научнотехнической информации.	Этапы: - проектно-конструкторский, - доклад по результатам самостоятельной работы по теме практики.	ФОС: Выполненное на практике задание.
	Владеть - методиками саморазвития, самостоятельного приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков.	Этап – проектно-конструкторский	ФОС: текст доклада и презентация по результатам самостоятельной работы на практике, собеседование на защите отчета по практике.
ПК-6 способность участвовать в разработке проектной и технической документации	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации; - программные и аппаратные средства обеспечения безопасности ОС, баз данных, сетевой безопасности.	Этапы: - проектно-конструкторский, - доклад по результатам самостоятельной работы по теме практики.	ФОС: Выполненное на практике задание.
	Уметь - определять информационную структуру и информационные ресурсы орга-		ФОС: Собеседование по тексту отчета по практике.

	<p>низации, подлежащие защите;</p> <ul style="list-style-type: none"> - разрабатывать организационно-распорядительные и нормативно-технические документы, регулирующие обеспечение информационной безопасности в организации. 		
<p>ПК-7 способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем</p>	<p>Владеть</p> <ul style="list-style-type: none"> - методами формирования требований по защите информации; - навыками разработке проектной и технической документации. <p>Знать</p> <ul style="list-style-type: none"> - основные методы управления информационной безопасностью; - организацию работы и нормативные правовые акты по аттестации объектов информатизации; - методы и средства контроля эффективности технической и программной защиты информации; - средства и методы предотвращения и обнаружения вторжений. <p>Уметь</p> <ul style="list-style-type: none"> - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем. - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем. <p>Владеть</p> <ul style="list-style-type: none"> - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - навыками участия в экспертизе состояния защищенности информации на объекте защиты. 	<p>Этапы:</p> <ul style="list-style-type: none"> - проектно-конструкторский, - доклад по результатам самостоятельной работы по теме практики. 	<p>ФОС: Выполненное на практике задание.</p> <p>ФОС: Выполненное на практике задание.</p> <p>ФОС: Отзыв руководителя практики.</p>

ПК-8 способность участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знать - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - методы и средства контроля эффективности технической защиты информации; - основные методы управления информационной безопасностью.	Этапы: - проектно-конструкторский, - доклад по результатам самостоятельной работы по теме практики.	ФОС: Выполненное на практике задание.
	Уметь - оценивать информационные риски в информационных системах; - формулировать и настраивать политику безопасности основных ОС; - использовать средства защиты, предоставляемые СУБД; - осуществлять меры противодействия нарушениям сетевой безопасности.		ФОС: Выполненное на практике задание.
	Владеть - методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации; - навыками разработки программных модулей, реализующих задачи, связанные с обеспечением информационной безопасности.		ФОС: Отзыв руководителя практики.
ПК-15 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать - методы и средства контроля эффективности технической защиты информации; - методы организации и управления деятельностью служб защиты информации на предприятии; - организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в	Этапы: - проектно-конструкторский, - доклад по результатам самостоятельной работы по теме практики.	ФОС: текст доклада и презентация по результатам самостоятельной работы на практике.

	области обеспечения государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты.		
	Уметь - анализировать текущее состояние ИБ на предприятии с целью разработки требований к процессам управления ИБ.		ФОС: Выполненное на практике задание.
	Владеть - навыками выбора и обоснования критериев эффективности функционирования защищенных систем.		

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 14. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Порядок представления отчетности по практике

Для аттестации студент предъявляется дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях А, Б, В.

Производственная технологическая и эксплуатационная практика**Цели производственной технологической и эксплуатационной практики.**

Приобретение практических навыков и компетенций в сфере технологической и эксплуатационной деятельности по обеспечению информационной безопасности на базе профильного предприятия (организации).

Задачи производственной технологической и эксплуатационной практики.

Основными задачами производственной технологической эксплуатационной практики являются:

– изучение современных информационных технологий, применяемых в производственном процессе, специального программного обеспечения и оборудования для решения задач по анализу защищенности объекта информатизации;

– ознакомление студентов с правилами эксплуатации и особенностей применяемого в профильной организации оборудования, с действующими стандартами, положениями и инструкциями по деятельности подразделения;

– приобретение практических знаний и умений по установке, настройке, эксплуатации и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований, администрирование подсистем информационной безопасности объекта;

– приобретение практического опыта участия в проведении аттестации объектов информатизации по требованиям безопасности информации и в аудите информационной безопасности автоматизированных систем, составления необходимых инструкций, проведения оценки соответствия выполненной работы техническому заданию и действующим нормативным документам.

Время проведения производственной технологической и эксплуатационной практики

6 курс, В семестр

Содержание производственной технологической и эксплуатационной практики

Общая трудоемкость производственной технологической эксплуатационной практики: общая трудоемкость производственной эксплуатационной практики составляет 3 зачетные единицы, 180 часов.

Разделы (этапы) практики:

подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ;

эксплуатационно-технологический этап: изучение нормативных документов по защите информации и методики проверки защищенности объекта информатизации; принципов формирования политики информационной безопасности в корпоративной информационной системе; оценки информационных рисков в информационной системе; знакомство с применяемыми в организации принципами технического, программного и информационного обеспечения защищенных информационных систем, методами и средствами обеспечения сетевой безопасности; безопасности операционных систем; безопасности в СУБД; приобретение практических знаний и умений по установке, настройке, эксплуатации и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; администрирование подсистем информационной безопасности объекта, участия в проведении аттестации объектов информатизации по требованиям безопасности информации и в аудите информационной безопасности автоматизированных систем, составления необходимых инструкций, проведения оценки соответствия выполненной работы техническому заданию и действующим нормативным документам; разработка своих предложений по совершенствованию системы управления информационной безопасностью в организации.

этап - оформление отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Научно-исследовательские и научно-производственные технологии, используемые на производственной практике. При прохождении производственной практики работа студента подразумевает практическое использование средств вычислительной техники, специального программного обеспечения и оборудования для анализа защищенности объекта информатизации, а также изучение различных информационных технологий, стандартов в области информационной безопасности объектов и систем.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

– способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

– способность к самоорганизации и самообразованию (ОК-8);

Профессиональные компетенции (ПК):

– способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

– способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное

обеспечение (ПК-17);

- способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств, обеспечение информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18);

- способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа (ПК-14).

Формы промежуточной аттестации (по итогам практики).

зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 15. Перечень фонда оценочных средств производственной технологической и эксплуатационной практике

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики. Приложение К.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с.<URL:http://www.methodolog.ru/books/mni.pdf>
3	Митрофанова Е.Ю., Сирота А.А. Методические указания по оформлению выпускных работ бакалавров / Е.Ю., Митрофанова, А.А. Сирота, учебно-методическое пособие, - Воронеж: Издательский дом ВГУ, 2016 – 23 с.
4	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
5	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное по-

	собие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
7	Фостер, Джеймс. Защита от взлома: сокет, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
9	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
10	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виера ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
11	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. — СПб. : БХВ-Петербург, 2006. - 304 с.
12	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.
13	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

б) дополнительная литература:

№ п/п	Источник
14	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
15	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. — Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
16	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 — Загл. с экрана.
17	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. — 2010.— Вып. 20. — № 2. — 350 с.
18	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
19	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Со-

	брание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
20	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
21	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
22	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
23	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
24	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Сборник законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
25	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
26	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Сборник законодательства Воронежской области 20.06.2011 № 4, ст. 285.
27	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
28	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
29	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
30	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
31	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
32	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
33	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.

34	Андрианов В.И. "Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
35	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
36	Брусницын Н.А. Открытость и шпионаж / Н.А.Брусницын. – М.: Воениздат, 1991.
37	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
38	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
39	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
40	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
41	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
42	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
43	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
44	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
45	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный. - Загл. с экрана.
46	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых. — Воронеж : ИПЦ ВГУ, 2008. — 95 с. : ил. — Библиогр.: с.95. — <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf >
47	Портал государственных услуг Российской Федерации www.gosuslugi.ru
48	http://www.cryptopro.ru
49	http://www.infotecs.ru
50	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows.Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич,ООО "ЛИССИ". Источник: RSDN Magazine #3-2006
51	http://www.lissi-crypto.ru/
52	http://www.signal-com.ru
53	http://www.shipka.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы на конференции по итогам практики. Проводится собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов приведен в ФОС (Приложение К).

Контрольные вопросы - типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения производственной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы производственной технологической и эксплуатационной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практики в рамках выполнения самостоятельной работы на месте прохождения практики под руководством руководителя практики от кафедры (Табл.16).

Таблица 16. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-6 способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знать - научные основы, цели, принципы, методы и технологии управленческой деятельности; - принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов.	Этап - выполнение эксплуатационно-технологических работ	Собеседование по вопросам ФОС для курса Основы управленческой деятельности.
	Уметь - работать в коллективе, принимать управленческие решения и оценивать их эффективность. - работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия.		Ответы на вопросы по отчету по практике. Отзыв руководителя практики.
	Владеть - навыками общения с коллегами при решении про-		

<p>ОК-8 способность к самоорганизации и самообразованию</p>	<p>изводственных задач.</p> <p>Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам.</p> <p>Уметь - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации.</p> <p>Владеть - методиками саморазвития, самостоятельного приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков.</p>	<p>Этапы: - выполнение эксплуатационно-технологических работ, - оформления отчёта по результатам самостоятельной работы по теме практики.</p>	<p>ФОС: Собеседование по тексту отчета по практике.</p> <p>ФОС: выполненное в ходе прохождения практики задание.</p> <p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>
<p>ПК-5 способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>	<p>Знать - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - защитные механизмы и средства обеспечения сетевой безопасности; - защита в операционных системах; - средства и методы предотвращения и обнаружения вторжений; - способы и средства защиты информации от утечки по техническим каналам.</p> <p>Уметь - формулировать и настраивать политику безопасности основных ОС, а так же локальных компьютерных сетей, построенных на их основе; - использовать средства</p>	<p>Этап - выполнение эксплуатационно-технологических работ.</p>	<p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>

	<p>защиты, представляемые СУБД;</p> <ul style="list-style-type: none"> - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях. <p>Владеть</p> <ul style="list-style-type: none"> - навыками конфигурирования и администрирования ОС; - методиками анализа системного трафика; - методиками анализа результатов работы средств обнаружения вторжений; - навыками настройки межсетевых экранов. 		
<p>ПК-17</p> <p>способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных¹ сетевое программное обеспечение</p>	<p>Знать</p> <ul style="list-style-type: none"> - виды информационного взаимодействия и обслуживания; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации; - основные задачи, понятия, математические методы и алгоритмы криптографии. <p>Уметь</p> <ul style="list-style-type: none"> - использовать программные и аппаратные средства ПК; - проводить анализ показателей качества сетей и систем связи; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием аппаратных и программных средств. <p>Владеть</p> <ul style="list-style-type: none"> - навыками безопасного использования технических средств в профессиональной деятельности. 	<p>Этап - выполнение эксплуатационно-технологических работ.</p>	<p>ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>
<p>ПК-18</p> <p>способность производить установку,</p>	<p>Знать</p> <ul style="list-style-type: none"> - программно-аппаратные средства вычислительной 	<p>Этап - выполнение эксплуатационно-технологических ра-</p>	<p>ФОС: Текст доклада и презентация по результатам</p>

<p>наладку, тестирование и обслуживание современных программно-аппаратных средств, обеспечение информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p>	<p>техники;</p> <ul style="list-style-type: none"> - защитные механизмы и средства обеспечения сетевой безопасности; - методы защиты в операционных системах; - средства и методы предотвращения и обнаружения вторжений; - основные задачи, понятия, математические методы и алгоритмы криптографии; - средства защиты, представляемые СУБД. <p>Уметь</p> <ul style="list-style-type: none"> -проводить анализ показателей качества сетей и систем связи; - производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств, обеспечение информационной безопасности; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием аппаратных и программных средств. <p>Владеть</p> <ul style="list-style-type: none"> - методами мониторинга и аудита угроз информационной безопасности информационных систем; - навыками безопасного использования технических средств в профессиональной деятельности. 	<p>бот.</p>	<p>самостоятельной работы на практике. Собеседование на защите отчета по практике.</p>
<p>ПК-14 способность организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа</p>	<p>Знать</p> <ul style="list-style-type: none"> - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - методы и средства контроля эффективности технической защиты информации; - отечественные и зарубежные стандарты в области компьютерной безопасности. 	<p>Этапы:</p> <ul style="list-style-type: none"> - выполнение эксплуатационно-технологических работ, - оформления отчёта по результатам самостоятельной работы по теме практики. 	<p>ФОС: Собеседование по тексту отчета по практике.</p>

	<p>Уметь</p> <ul style="list-style-type: none"> - оценивать информационные риски в информационных системах; - разрабатывать проекты нормативных документов и организационно-распорядительных документов, регламентирующих работу по защите информации. 	<p>Этап - выполнение эксплуатационно-технологических работ.</p>	
	<p>Владеть</p> <ul style="list-style-type: none"> - методами управления информационной безопасностью информационных систем; - методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации. 	<p>Этап - выполнение эксплуатационно-технологических работ.</p>	<p>Ответы на вопросы по отчету по практике. Отзыв руководителя практики.</p>

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 16. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Порядок представления отчетности по практике

Для аттестации студент предъявляется дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях А, Б, В.

Производственная преддипломная практика

Цели производственной преддипломной практики:

– систематизацию, расширение и закрепление и углублению теоретических профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки;

– формирование у студентов навыков ведения самостоятельной научной работы, исследования и экспериментирования;

– овладение необходимыми профессиональными компетенциями по избранному направлению специализированной подготовки.

Задачи производственной преддипломной практики

Основной задачей производственной преддипломной практики является приобретение опыта в исследовании актуальной научной проблемы, а также подбор необходимых материалов для выполнения выпускной квалификационной работы.

Во время научно-исследовательской практики студент должен:

изучить:

– информационные источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;

– методы моделирования и исследования вопросов информационной безопасности;

– методы анализа и обработки данных, являющихся входными для проведения научного исследования;

- информационные технологии, применяемые в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;
- требования к оформлению научно-технической документации;

выполнить:

- анализ, систематизацию и обобщение информации по теме исследований;
- сравнение результатов исследования объекта разработки с отечественными и зарубежными аналогами;
- анализ научной и практической значимости проводимых исследований.

Время проведения производственной преддипломной практики

4 курс, 8 семестр.

Содержание производственной преддипломной практики

Общая трудоемкость производственной преддипломной практики составляет 5 зачетных единиц, 180 час.

Разделы (этапы) практики.

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ.

Научно-исследовательский этап: выбор темы исследования; определение проблемы, объекта и предмета исследования; формулирование цели и задач исследования; теоретический анализ литературы и исследований по проблеме, подбор необходимых источников по теме (патентные материалы, научные отчеты, техническая документация и др.); составление библиографии; формулирование рабочей гипотезы.

Этап выполнения исследовательских работ по индивидуальному плану: формулирование цели и задач исследования, проведение обзора и выбор современных информационных технологий, специального программного обеспечения и оборудования для решения поставленной задачи по анализу защищенности объекта информатизации; проведение самостоятельного решения учебной научной задачи, исследований и экспериментов.

Этап оформления отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

устный доклад по результатам самостоятельной работы по теме практики на итоговой студенческой конференции.

Научно-исследовательские и научно-производственные технологии, используемые на производственной преддипломной практике. При прохождении производственной преддипломной практики работа студента подразумевает практическое использование средств вычислительной техники, специального программного обеспечения и оборудования для анализа защищенности объекта информатизации, а также изучение различных информационных технологий, стандартов в области информационной безопасности объектов и систем.

Результаты освоения, коды формируемых (сформированных) компетенций

Общекультурные компетенции (ОК):

- способность к самоорганизации и самообразованию (ОК-8)

Общепрофессиональные компетенции (ОПК):

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными

проектами (ОПК-4).

Формы промежуточной аттестации (по итогам практики)

зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 17. Перечень фонда оценочных средств производственной преддипломной практики

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос Собеседование	Вопросы по темам/разделам практики. Приложение И, К.	Шкалы оценивания приведены в разделе – “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”
2	Практическое задание	Соответствует заданию на практику	Шкалы оценивания приведены в разделе - “Описание шкалы, показателей и методика оценивания степени сформированности компетенций, полученных в результате прохождения практики”

Список учебных пособий и методических рекомендаций

а) основная литература:

№ п/п	Источник
1	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>
2	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с.<URL:http://www.methodolog.ru/books/mni.pdf>
3	Митрофанова Е.Ю., Сирота А.А. Методические указания по оформлению выпускных работ бакалавров / Е.Ю., Митрофанова, А.А. Сирота, учебно-методическое пособие, - Воронеж: Издательский дом ВГУ, 2016 – 23 с.
4	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
5	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
7	Фостер, Джеймс. Защита от взлома: сокет, эксплойты, shell-код : / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность) .— .— ISBN 5-9706-0019-9 : 449.10 p. —

	<URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите : / Э. Скудис .— Москва : ДМК Пресс, 2009 .— 512 с. : ил. — (Защита и администрирование) .— .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
9	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
10	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
11	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.
12	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.
13	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

б) дополнительная литература:

№ п/п	Источник
14	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва : Флинта : Наука, 2014. — 108 с.
15	Кручинин, В.В. Компьютерные технологии в научных исследованиях : учебно-методическое пособие / В.В. Кручинин. – Москва : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269 — Загл. с экрана.
16	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В.Барвиненко, В.С. Верба. — Москва : Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348 — Загл. с экрана.
17	Системы и средства информатики : Ежегодник / Гл. ред. И.А. Соколов. — Москва : ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
18	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
19	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
20	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)
21	Приказ Федеральной службы по техническому и экспортному контролю России от 11

	февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
22	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
23	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
24	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
25	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
26	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
27	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
28	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
29	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
30	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
31	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII междунар. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
32	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
33	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
34	Андреанов В.И. "Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
35	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
36	Брусницин Н.А. Открытость и шпионаж / Н.А.Брусницин. – М.: Воениздат, 1991.
37	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.

38	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
39	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
40	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
41	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
42	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
43	Электронная библиотека рабочих учебных программ дисциплин. Режим доступа: http://smwww.main.vsu.ru
44	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
45	Фундаментальные и прикладные исследования в области параллельных вычислений [электр. ресурс]. – Режим доступа http://parallel.ru/research свободный. - Загл. с экрана.
46	Элементы теории чисел и криптозащита : учебное пособие для вузов. Ч. 2 / Воронеж. гос. ун-т; сост.: Б.Н. Воронков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 95 с. : ил. — Библиогр.: с.95 .— <URL: http://www.lib.vsu.ru/elib/texts/method/vsu/m08-238.pdf >
47	Портал государственных услуг Российской Федерации www.gosuslugi.ru
48	http://www.cryptopro.ru
49	http://www.infotecs.ru
50	http://www.rsdn.ru/article/crypto/cspsecrets.xml Секреты разработки CSP для Windows.Создание криптографического провайдера для Windows. Зырянов Юрий Сергеевич,ООО "ЛИССИ". Источник: RSDN Magazine #3-2006
51	http://www.lissi-crypto.ru/
52	http://www.signal-com.ru
53	http://www.shipka.ru

Критерии оценивания результатов практики

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы на конференции по итогам практики. Проводится собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень вопросов и заданий приведен в ФОС (Приложение И, К).

Контрольные вопросы и задания - типовые, однако ответы на них должны иметь конкретную информацию, обусловленную индивидуальным заданием на практику.

При выведении оценки должны учитываться не только качество выполненного задания, ответы студента на теоретические вопросы, но и вся деятельность в период прохождения учебной практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы производственной преддипломной практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего периода прохождения практики в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры (Табл.18).

Таблица 18. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-8 способность к самоорганизации и самообразованию	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам. <p>Уметь</p> <ul style="list-style-type: none"> - ориентироваться в условиях избытка информации, способность выделять ключевые приоритеты и следовать им; - пользоваться современными источниками научно-технической информации. <p>Владеть</p> <ul style="list-style-type: none"> - методиками саморазвития, самостоятельно приобретения и освоения новых знаний; - навыками критической оценки своих достоинств и недостатков; - опытом выбора средств и возможностей развития достоинств и устранения недостатков. 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - выполнения исследовательских работ по индивидуальному плану. 	ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике.
ОПК-2 способность корректно применять при решении профессио-	<p>Знать</p> <ul style="list-style-type: none"> - основные понятия и методы математического анализа, аналитиче- 	<p>Этапы:</p> <ul style="list-style-type: none"> - научно-исследовательский, - выполнения иссле- 	ФОС: Текст доклада и презентация по результатам самостоятельной работы

<p>нальных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов</p>	<p>ской геометрии, линейной алгебры, теории комплексного переменного;</p> <ul style="list-style-type: none"> - методы математической статистики и теории вероятностей; - математические методы обработки экспериментальных данных; - математический аппарат дискретной математики, числовых методов. <p>Уметь</p> <ul style="list-style-type: none"> - использовать математические методы и модели для решения прикладных задач; - строить математические модели задач профессиональной области. <p>Владеть</p> <ul style="list-style-type: none"> - методами количественного анализа процессов обработки, поиска и передачи информации; - навыками использования математического аппарата в экспериментальных исследованиях. 	<p>довательских работ по индивидуальному плану.</p>	<p>на практике.</p>
<p>ОПК-4 способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p>	<p>Знать</p> <ul style="list-style-type: none"> - основные методы обобщения, восприятия и анализа информации; - методы анализа причинно-следственных связей; - основные естественнонаучные законы, применение математического аппарата для решения профессиональных задач; - методы программирования и методы разработки эффективных алгоритмов решения прикладных задач. <p>Уметь</p> <ul style="list-style-type: none"> - выявлять сущность проблем, возникающих 	<p>Этап - исследовательских работ по индивидуальному плану.</p>	<p>ФОС: Собеседование, анализ выполнения практического задания.</p>

	в ходе профессиональной деятельности; - формулировать результат проведенных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области.		
	Владеть - профессиональной терминологией; - навыками применения современных методов научных исследований; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.	Этап - оформления отчёта.	Собеседование на защите отчета по практике.

Описание шкалы, показателей и методика оценивания степени сформированности компетенций (результатов обучения), полученных в результате прохождения практики

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице 18. Формирование этих дескрипторов происходит в течение всего периода прохождения производственной преддипломной практики, в рамках выполнения самостоятельной работы под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

– требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

– результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

– результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

– результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие

вета, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

– выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

– выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

– выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

– требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Порядок представления отчетности по практике

Для аттестации студент предъявляется дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложении А, Б, В.

ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ



Э.К. Алгазинов

**Приложение Б
(обязательное)**

Форма отчета обучающегося о прохождении практики

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
“ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”
(ФГБОУ ВО «ВГУ»)

Факультет компьютерных наук

Кафедра технологий обработки и защиты информации

Отчет по _____ практике

указать вид практики

<Тема практики>

Специальность 10.05.01 Компьютерная безопасность

Специализация «Анализ безопасности компьютерных систем»

Зав. кафедрой _____ . ____ .20__
Подпись, расшифровка, ученая степень, звание

Обучающийся _____ . ____ .20__
Подпись, расшифровка подписи

Руководитель практики от ВГУ _____ . ____ .20__
Подпись, расшифровка подписи, ученая степень, звание

Руководитель практики от предприятия _____ . ____ .20__
Подпись, расшифровка подписи, ученая степень, звание

Воронеж 20__

Приложение В (обязательное)

СТРУКТУРА ОТЧЕТА ПО ПРАКТИКЕ

1. Отчет по практике должен включать титульный лист, содержание, введение, описание теоретических и практических аспектов выполненной работы, заключение, список использованных источников, приложения.

2. На титульном листе должна быть представлена тема практики, группа и фамилия студента, данные о предприятии, на базе которого выполнялась практика, фамилия руководителя.

3. Во введении студенты должны дать краткое описание задачи, решаемой в рамках практики.

4. В основной части отчета студенты приводят подробное описание проделанной теоретической и (или) практической работы, включая описание и обоснование выбранных решений, описание программ и т.д.

5. В заключении дается краткая характеристика проделанной работы, и приводятся ее основные результаты.

6. В приложениях приводятся непосредственные результаты разработки: тексты программ, графики и диаграммы, и т.д.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА

1. Отчет оформляется в печатном виде, на листах формата А4.

2. Основной текст отчета выполняется шрифтом 13-14 пунктов, с интервалом 1,3-1,5 между строками. Текст разбивается на абзацы, каждый из которых включает отступ и выравнивание по ширине.

3. Текст в приложениях может быть выполнен более мелким шрифтом.

4. Отчет разбивается на главы, пункты и подпункты, включающие десятичную нумерацию.

5. Рисунки и таблицы в отчете должны иметь отдельную нумерацию и названия.

6. Весь отчет должен быть оформлен в едином стиле: везде в отчете для заголовков одного уровня, основного текста и подписей должен использоваться одинаковый шрифт.

7. Страницы отчета нумеруются, начиная с титульного листа. Номера страниц проставляются в правом верхнем углу для всего отчета кроме титульного листа.

8. Содержание отчета должно включать перечень всех глав, пунктов и подпунктов, с указанием номера страницы для каждого элемента содержания.

9. Ссылки на литературу и другие использованные источники оформляются в основном тексте, а сами источники перечисляются в списке использованных источников.

10. Объем отчета по практике должен быть не менее 20 страниц.

**Приложение Г
(рекомендуемое)**

**Список вопросов для проведения собеседования по
учебной ознакомительной практике**

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра технологий обработки и защиты информации

**Список вопросов для проведения собеседования
по учебной ознакомительной практике**

Б2.У.1 Учебная ознакомительная практика

1. Понятие информационной безопасности.
2. Принципы построения систем защиты информации.
3. Актуальность проблемы обеспечения безопасности в информационном обществе.
4. Средства обеспечения информационной безопасности в корпоративных информационных системах
5. Аппаратные средства обеспечения информационной безопасности
6. Информационные уязвимости объектов
7. Программные средства обеспечения информационной безопасности
8. Антропогенные информационные уязвимости
9. Техногенные информационные уязвимости
10. Организационно-правовые средства обеспечения информационной безопасности
11. Угрозы информационной безопасности и их источники
12. Организационно-административные средства защиты информации
13. Основные причины утечки информации.
14. Политика безопасности. Основные типы политики безопасности.
15. Меры защиты персональных данных в информационных системах.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;
- оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;

- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.

**Приложение Д
(рекомендуемое)**

**Перечень вопросов для проведения собеседования на защите отчета
по учебно-лабораторному практикуму**

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра вычислительной математики и
прикладных информационных технологий

**Перечень вопросов для проведения собеседования на защите отчета
по учебно-лабораторному практикуму**

Б2.У.2. Учебно-лабораторный практикум

1. LU-разложение матрицы.
2. Метод Гаусса решения систем линейных уравнений.
3. Метод прогонки.
4. Построение интерполяционного многочлена методом неопределённых коэффициентов.
5. Интерполяционный многочлен Лагранжа.
6. Интерполяционный многочлен Ньютона.
7. Метод наименьших квадратов.
8. Приближение функции кубическими сплайнами.
9. Метод простых итераций. Метод Ньютона. Метод секущих.
10. Явный метод Эйлера. Неявный метод Эйлера.
11. Методы Рунге – Кутты.
12. Методы приближённого решения краевых задач для обыкновенных дифференциальных уравнений второго порядка.
13. Простейшие явная и неявная разностные схемы в случае задачи Коши для уравнения теплопроводности.
14. Разностная схема «крест» в случае начально-краевой задачи для волнового уравнения.
15. Разностная схема «крест» в случае задачи Дирихле для уравнения Пуассона.
16. Дискретное преобразование Фурье. Быстрое преобразование Фурье.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;
- оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;

- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.

Приложение Е
(рекомендуемое)

Перечень заданий для проведения учебно-лабораторного практикума

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра вычислительной математики и
прикладных информационных технологий

Перечень заданий для проведения учебно-лабораторного практикума

Б2.У.2. Учебно-лабораторный практикум

Задание №1.

Найти максимальное по модулю собственное значение степенным методом для заданной матрицы.

Задание №2.

С помощью LU-разложения найти собственные значения и собственные вектора для заданной матрицы.

Задание №3.

Методом Халецкого решить систему линейных алгебраических уравнений с ленточной матрицей.

Задание №4.

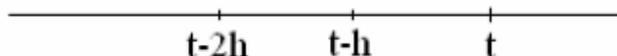
Вычислить интерполяционное значение функции и оценить точность полученного значения с использованием полиномов Лагранжа второй и третьей степени.

Задание №5.

Интерполировать функции с помощью многочлена Лагранжа степени m на неравномерной сетке узлов.

Задание №6.

Построить сеточное приближение $u'(t)$ 2-го порядка точности с шаблоном



Задание №7.

Решить нелинейное дифференциальное уравнение методом хорд (методом линейной интерполяции)

Задание №8.

Решить систему нелинейных дифференциальных уравнений методом половинного деления.

Задание №9.

Решить явным методом Эйлера задачу Коши для системы обыкновенных дифференциальных уравнений с заданной точностью, используя для выбора шага сетки правило Рунге.

Задание №10.

Сравнить метод Рунге-Кутты и метод Адамса заданного порядка точности.

**Приложение Ж
(рекомендуемое)**

Список вопросов для проведения собеседования по учебной практике по получению первичных профессиональных умений и навыков

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра технологий обработки и защиты информации

Список вопросов для проведения собеседования по учебной практике по получению первичных профессиональных умений и навыков

Б2.У.3 Учебная практика по
получению первичных профессиональных умений и навыков

1. Понятие информационной безопасности.
2. Принципы построения систем защиты информации.
3. Актуальность проблемы обеспечения безопасности в информационном обществе.
4. Средства обеспечения информационной безопасности в корпоративных информационных системах
5. Аппаратные средства обеспечения информационной безопасности
6. Информационные уязвимости объектов
7. Программные средства обеспечения информационной безопасности
8. Антропогенные информационные уязвимости
9. Техногенные информационные уязвимости
10. Организационно-правовые средства обеспечения информационной безопасности
11. Угрозы информационной безопасности и их источники
12. Организационно-административные средства защиты информации
13. Основные причины утечки информации.
14. Политика безопасности. Основные типы политики безопасности.
15. Меры защиты персональных данных в информационных системах персональных данных.
16. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения ИБ.
17. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
18. Методы и средства обеспечения ИБ компьютерных систем.
19. Подтверждение подлинности объектов и субъектов информационной системы.
20. Контроль целостности информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;
- оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;
- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.

**Приложение 3
(рекомендуемое)**

**Список вопросов для проведения собеседования
по учебной экспериментально-исследовательской практике**

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра технологий обработки и защиты информации

**Список вопросов для проведения собеседования
по учебной экспериментально-исследовательской практике**

Б2.У.4. Учебная экспериментально-исследовательская практика

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
10. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
11. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
12. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
13. Биометрические средства идентификации и аутентификации пользователей.
14. Аутентификация субъектов в распределенных системах, проблемы и решения.

15. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
16. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
17. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
18. Физические средства обеспечения информационной безопасности.
19. Средства обеспечения информационной безопасности в ОС

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;
- оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;
- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.

**Приложение И
(рекомендуемое)**

**Список вопросов для проведения собеседования по
производственной конструкторской практике**

**МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)**

Кафедра технологий обработки и защиты информации

**Список вопросов и заданий для проведения собеседования по результатам
производственной конструкторской практики**

Б2.П.2 Производственная конструкторская практика

**Примерный список заданий для студентов по производственной
конструкторской практике**

1. Автоматизированная система в защищенном исполнении организации (или предприятия любой формы собственности).
2. Анализ уязвимостей и организация защиты информации в локальной сети организации (или предприятия любой формы собственности).
3. Анализ уязвимостей и эффективности средств и способов защиты информации в автоматизированной системе организации (или предприятия любой формы собственности).
4. Инструментальный мониторинг защищенности автоматизированной системы организации (или предприятия любой формы собственности).
5. Информационная система персональных данных организации (или предприятия любой формы собственности).
6. Комплексная защита информации в локальной сети организации (или предприятия любой формы собственности).
7. Подготовка к аттестации информационной системы персональных данных в организации (или предприятии любой формы собственности).
8. Сбор и анализ исходных данных для проектирования системы защиты информации организации (или предприятия любой формы собственности).
9. Система контроля и управления доступом в организации (или на предприятии любой формы собственности).
10. Система управления информационной безопасностью автоматизированной системы организации (или предприятия любой формы собственности).

**Список теоретических вопросов по производственной
конструкторской практике**

1. Понятие политики безопасности информационных систем. Назначение политики безопасности.

2. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
3. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
4. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
5. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
6. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
7. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
8. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
9. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
10. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
11. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
12. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
13. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
14. Биометрические средства идентификации и аутентификации пользователей.
15. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
16. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
17. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
18. Законодательный уровень применения цифровой подписи.
19. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
20. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
21. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
22. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
23. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
24. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.

25. Разграничение доступа к данным в ОС семейства UNIX.
26. Пользователи и группы в ОС UNIX.
27. Пользователи и группы в ОС Windows.
28. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
29. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
30. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
31. Распределенные информационные системы. Удаленные атаки на информационную систему.
32. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
33. Физические средства обеспечения информационной безопасности.
34. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
35. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
36. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
37. Виртуальные частные сети, их функции и назначение.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;
- оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;
- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.

**Приложение К
(рекомендуемое)**

Список вопросов для проведения собеседования на защите отчета по производственной технологической и эксплуатационной практике

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

Кафедра технологий обработки и защиты информации

Список вопросов для проведения собеседования на защите отчета по производственной технологической и эксплуатационной практике

Б2.П.3. Производственная технологическая и эксплуатационная практика

Теоретические вопросы профессиональной направленности

1. Основные методы и средства защиты информационных систем.
2. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы.
3. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).
4. Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб.
5. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности.
6. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности.
7. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.
8. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
9. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.
10. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны.
11. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.
12. Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.
13. Причины нарушения безопасности информации при ее обработке СКЗИ.
14. Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности.

15. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации.

16. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

17. Международные стандарты информационной безопасности.

18. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования.

19. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

Вопросы практической направленности

1. Какова структура подразделения, в которой проходила практика?
2. Охарактеризуйте должностные обязанности работников подразделения.
3. Перечислите методы защиты конфиденциальной информации в подразделении, в котором проходила производственная практика.
4. Укажите порядок защиты речевой информации.
5. Перечислите действия, предпринимаемые для защиты автоматизированных систем от несанкционированного доступа, на предприятии, на котором проводилась практика.
6. Проанализируйте состояния баз данных подразделения на предмет обеспечения информационной безопасности.
7. Перечислите нормативно-правовую документацию, которая имеется на предприятии для обеспечения информационной безопасности.
8. Какие программы или комплексы по защите информации Вы рассматривали на практике? Каким образом установить и настроить эти программы? Как поддерживаются они в работоспособном состоянии?
9. Каким образом обеспечивается совместимость программных продуктов?
10. Как организовано администрирование подсистем информационной безопасности?
11. Что такое электронно-цифровая подпись? На каких алгоритмах могут они базироваться? Как создать ЭЦП?
12. Анализ каких объектов информационной безопасности Вы проводили на практике?
13. Какие документы, применяемые в технологической документации, Вы рассматривали на практике?
14. Какие знания, умения и навыки были Вами приобретены в результате прохождения практики?

Критерии оценки:

– оценка «отлично» выставляется студенту, если ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный;

– оценка «хорошо» ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки;

- оценка «удовлетворительно» при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный;
- оценка «неудовлетворительно» неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия.