www.vsu.ru

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

П ВГУ 2.1.02.100301Б – 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 направлению подготовки
10.03.01 Информационная безопасность

Профиль «Безопасность компьютерных систем»
Бакалавриат

РАЗРАБОТАНО – рабочей группой факультета компьютерных наук

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

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

ВВЕДЕНО В ДЕЙСТВИЕ приказом ректора 30.12.2016 № 1118

ВВОДИТСЯ ВЗАМЕН П ВГУ 2.1.02.100301Б – 2016

СРОК ПЕРЕСМОТРА при изменении ФГОС

1 Область применения

Настоящее Положение обязательно для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (профиль «Безопасность 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 направлению подготовки 10.03.01 Информационная безопасность, утвержденный приказом Министерства образования и науки Российской Федерации от 01.12.2016 г. № 1515;

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 направлению Информационная безопасность в практическую подготовку студентов входят следующие виды практик: учебная и производственная, в том числе преддипломная практики.

Типы учебной практики:

- учебная ознакомительная;
- учебная практика по получению первичных профессиональных умений и навыков;
- учебная технологическая.

По способу проведения учебные практики являются стационарными.

По форме проведения все типы учебных практик являются концентрированными.

Типы производственной практики:

- производственная проектно-технологическая;
- производственная эксплуатационная;
- преддипломная.

По способу проведения производственные практики являются стационарными.

По форме проведения производственная проектно-технологическая практика является рассредоточенной, остальные типы производственных практик являются концентрированными.

Учебная ознакомительная практика, учебная практика по получению первичных профессиональных умений и навыков, учебная технологическая практика проводятся кафедрой Технологий обработки и защиты информации, как в аудиторной, так и внеаудиторной формах. Место проведения практики – аудитории, компьютерные и специа-

лизированные лаборатории факультета компьютерных наук Университета, Управление информатизации и компьютерных технологий ВГУ (УИиКТ).

Производственная проектно-технологическая**,** производственная эксплуатационная и производственная преддипломная практики проводится на одном или нескольких профильных предприятиях (организациях, учреждениях фирмах), с которыми заключены договора на прохождение практики.

Учебная практика по получению первичных профессиональных умений и навыков, учебная технологическая практика и все виды производственных практик завершаются проведением итоговой конференции по результатам 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 предприятия (для производственных практик), форма отзыва руководителя от предприятия приведена Приложении А, выставляет оценку по 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.

Все виды и типы практик соответствуют видам деятельности, на которые направлена основная образовательная программа по направлению подготовки 10.03.01 Информационная безопасность: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

3.2. Общие требования к организации практик (по видам практик)

Согласно ФГОС ВО для направления подготовки 10.03.01 Информационная 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 направлению подготовки Информационная безопасность и настоящим Положением.

Учебная ознакомительная практика является первым звеном в цикле учебных практик в системе профессионального образования бакалавров, обучающихся по направлению Информационная безопасность. Она соответствует виду деятельности - организационно-управленческая. 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.

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 по направлению подготовки Информационная безопасность, - экспериментально-исследовательская. 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 технологическая практика является заключительным звеном в цикле учебных практик. Она ориентирована на два вида деятельности из четырех, на которые направлена образовательная программа: проектно-технологическую и экспериментально-исследовательскую деятельности. Учебная технологическая 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 проводятся на базе структурных подразделений Университета, научно-исследовательских институтов, аналитических центров в составе Университета.

Неотъемлемой частью процесса профессионального образования бакалавров, 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 проектно-технологическая практика. Она соответствует одному из видов деятельности, на которые ориентирована основная образовательная программа по направлению подготовки Информационная безопасность, как проектно-технологическая. Целями ее проведения являются: расширение теоретической подготовки, полученной в вузе, практическими знаниями; приобретение опыта самостоятельного решения практической проектно-технологической задачи. В процессе прохождения практики решается ряд задач: формирование у студентов умений и навыков проведения технологического обследования объекта информационной защиты; сбора экспериментального и экс-

пертного 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 проектно-технологической 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 эксплуатационная практика. Она ориентирована на вид деятельности - эксплуатационный. Данный тип практики направлен на приобретение практических навыков и компетенций в сфере профессиональной деятельности по обеспечению информационной безопасности, а также приобщение бакалавров к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций. Во время прохождение практики: воспитывается устойчивый интерес к профессии, убежденность в правильности ее выбора; развиваются потребности в самообразовании и самосовершенствовании профессиональных знаний и умения; формируется опыт творческой деятельности; формируются профессионально значимые качества личности будущего специалиста и его активной жизненной позиции.

Завершающим звеном в цепи производственных практик является - производственная преддипломная практика. Она ориентирована на два вида деятельности из четырех, на которые направлена образовательная программа: эксплуатационно-исследовательскую и проектно-технологическую. 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 производственная преддипломная 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 список 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.

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 общепрофессиональных 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 функционирование 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

1 курс, 2 семестр.

Содержание учебной ознакомительной 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;

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

Обще-профессиональные компетенции (ОПК):

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

Профессиональные компетенции:

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

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	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. Проводится 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 формирова-	Этапы формирования компетенции (разделы практики)	Форма отчетности практиканта, ФОС* (средства оценивания)

	ния знаний, умений, навыков)		
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.	Отчет по практике ФОС: Собеседование по вопросам Приложение Г.
	Уметь - пользоваться современной научно-технической 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 задание
ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать - основные угрозы информационной безопасности и модели нарушителя в информационных системах; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации	Этапы: - учебный ознакомительный, - оформление отчёта по итогам практики	ФОС: собеседование по вопросам ФОС для курса Б3.Б.1 Основы информационной безопасности
	Уметь - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем		ФОС: Собеседование, анализ выполнения практического задание
	Владеть - навыками анализа информационной инфраструктуры информационной системы и ее безопасности;		

	- методами выявления угроз информационной безопасности информационных систем		
ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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: - учебный ознакомительный, - оформление отчёта по итогам практики	ФОС: Собеседование по вопросам Приложение Г.
	Уметь - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем		ФОС: Собеседование по выполненным заданиям в процессе прохождения практики, тексту отчета.
	Владеть - методами управления информационной безопасностью информационных 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 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 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-ИП3, 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 задание руководителя на прохождение практики и оформляет результаты практики в виде отчета. Требования к оформлению отчета, форма отзыва руководителя представлены в Приложениях А, Б, В.

Учебная практика по получению первичных профессиональных умений и навыков

Цели учебной практики по получению первичных профессиональных умений и навыков

Целью учебной практика 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 студентом 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

2 курс, 3 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 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):

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

Профессиональные компетенции:

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

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

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

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. 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 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
ПК-11 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать - первичные сведений по обеспечению комплексной защиты информации в различных типах организаций; - основы правового регулирования обеспечения информационной безопасности; - назначение и классы специального программного обеспечения и оборудования для решения задач анализа защищенности объекта информатизации; - критерии оценки эффективности и надежности средств защиты программного и технического обеспечения информационных систем.	Этап - учебно-исследовательский	ФОС: по вопросам ФОС для курса - Основы информационной безопасности, вопросам Приложения Д.
	Уметь - анализировать и оценивать угрозы информаци-	Этап - учебно-исследовательский	ФОС: Собеседование, анализ выполнения практическо-

	онной безопасности объекта		го задание
	Владеть - методами проведения измерений, расчета и инструментального контроля показателей технической защиты информации	Этапы: - 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

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 4. 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 до-

статочно 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-ИП3, 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 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.

Учебная технологическая практика

Цели учебной технологической практики

Целью учебной технологической 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 технологической практики

Задачами учебной технологической 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 технологической 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 технологической практики

2 курс, 4 семестр.

Содержание учебной технологической 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-технологический 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; проведение самостоятельного решения учебной технологической 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 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

Профессиональные компетенции:

- способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК - 7);
- способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
- способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).

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 технологической 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 Е.	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	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>
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	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.
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, отзыва руководителя. Проводится собеседования по разделам отчета, анализируются ответы студентов на контрольные вопросы и задания. Перечень контрольных вопросов приведен в ФОС (Приложение Е).

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. 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)
ПК - 7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	Знать - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - методы и средства контроля эффективности технической защиты информации;	Этапы: - учебно-технологический, - выполнение индивидуального задания	ФОС: Собеседование, анализ выполнения практического задание

технико-экономического обоснования соответствующих проектных решений	- основные методы управления информационной безопасностью		
	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	Этап - оформления отчёта по итогам практики	
	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 осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей	Знать - основные методы обобщения, восприятия и анализа информации; - терминологию, принципы и основные направления обеспечения информационной безопасности. - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области	Этапы: - учебно-технологический, - выполнение индивидуального задания, - оформления отчёта.	ФОС: Собеседование на защите отчета по практике, вопросы Приложение Е.

профессиональной деятельности	информационной безопасности и защиты информации		
	Уметь - осуществлять сбор, обработку, анализ и систематизацию научно-технической информации.	Этап - оформления отчёта по итогам практики	
	Владеть - навыками работы с технической документацией на русском и иностранных языках; -методами обработки и анализа научно-технической информации по исследуемым проблемам и задачам.		
ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации	Этапы: - учебно-технологический, - выполнение индивидуального задания	ФОС: выполненное в ходе прохождения практики задание, вопросы к собеседованию Приложение Е.
	Уметь - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации		
	Владеть - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовыми актами по технической защите информации	Этап - оформление отчёта по итогам 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 6. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполне-

ния 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-ИП3, 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 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 проектно-технологическая практика

Цели производственной проектно-технологической практики

Целью производственной проектно-технологической практики является расширение теоретической подготовки, полученной в вузе, получение опыта проектной работы в профильных организациях и предприятиях, приобретение практических навыков и компетенций в сфере профессиональной деятельности по обеспечению информационной безопасности, а также приобщение бакалавров к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций.

Задачи производственной проектно-технологической практики

Задачами производственной проектно-технологической практики являются:

- формирование у студентов умений и навыков проведения технического обследования объекта информационной защиты: сбора экспериментального и экспертного материала и его теоретического обобщения, разработки технических предложений;
- формирование у студентов умений и навыков проведения технологического обследования объекта информационной защиты: сбора экспериментального и экспертного материала и его теоретического обобщения, разработки технических предложений;
- 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;

- приобретение опыта самостоятельного решения проектно-технологической задачи, проведение экспериментальных исследований, а также проведение предварительного технико-экономического обоснования проектных расчетов;

-выработка у студентов навыков разработки технологической и эксплуатационной документации;

- формирование у студентов навыков профессиональных взаимодействий с представителями организаций, проведения презентации результатов технических предложений, подготовки и оформления документации.

Время проведения производственной проектно-технологической практики

3 курс, 5 семестр.

Содержание производственной проектно-технологической практики

Общая трудоемкость производственной проектно-технологической практики составляет 2 зачетных единицы, 72 часа.

Разделы (этапы) практики:

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

этап выполнения проектных работ по индивидуальному заданию: 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 теоретического анализа 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; проведение самостоятельного решения учебной технологической задачи, исследований и экспериментов; разработка технических предложений;

этап - оформление отчёта по итогам практики: описание проделанной работы с самооценкой результатов 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 исследовательской практике. При прохождении производственной исследовательской 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

Профессиональные компетенции (ПК):

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

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

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 7. Перечень фонда оценочных средств по производственной проектно-технологической 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 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	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: 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. 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-x.

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 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	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 контрольных вопросов и примерных вариантов заданий приведен в ФОС (Приложение Ж).

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 практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», рас-

писанные 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.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)
ПК - 7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	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 - выполнения проектных работ по индивидуальному заданию	ФОС: Собеседование по вопросам ФОС для курса Основы информационной безопасности и вопросам из Приложения Ж.
	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	Этап - оформления отчёта по итогам практики	ФОС: Собеседование, анализ выполнения практического задание
	Владеть -методами управления информационной безопасностью информационных систем; - методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, про-		ФОС: Текст доклада и презентация по результатам самостоятельной работы по теме практики

	ведение экспериментальных исследований системы защиты информации; - методами оценки информационных рисков		
ПК-8 способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации	Этап – оформления отчёта по итогам практики	ФОС: Собеседование по вопросам Приложения Ж .
	Уметь - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации		ФОС: Текст доклада и презентация по результатам самостоятельной работы по теме практики, анализ выполнения практического задания
	Владеть - навыками работы с нормативными правовыми актами по технической защите информации		ФОС: Собеседование по тексту доклада.

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 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 эксплуатационная практика

Цели производственной эксплуатационной практики

Целями данной производственной эксплуатационной практики является закрепление и углубление теоретической подготовки, получение опыта производственной работы, приобретение практических навыков и компетенций в сфере профессиональной деятельности по обеспечению информационной безопасности, а также приобщение бакалавров к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций.

Задачи производственной эксплуатационной практики

Задачами производственной эксплуатационной практики являются:

- 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, эксплуатация 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 производственной эксплуатационной практики

3 курс, 6 семестр.

Содержание производственной эксплуатационной практики

Общая трудоемкость производственной исполнительской практики составляет 5 зачетных единиц, 180 часов.

Разделы (этапы) практики:

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

этап выполнения производственных эксплуатационных работ по индивидуальному плану*:* изучение нормативных документов по защите информации и методики проверки защищенности объекта информатизации; знакомство с принципами формирования политики информационной безопасности в корпоративной информационной системе; оценка 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, эксплуатация 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:

- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- способностью к самоорганизации и самообразованию (ОК-8);

Профессиональные компетенции:

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

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

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

Формы промежуточной аттестации (по итогам практики).

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 9. Перечень фонда оценочных средств производственной 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 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	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: 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. 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-x.

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 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	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 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. 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 учебной 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.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 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	Этап - выполнение производственных эксплуатационных работ	Собеседование по вопросам ФОС для курса Основы управленческой деятельности
	Уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность.		Ответы на вопросы по отчету по практике. Отзыв руководителя практики
	Владеть навыками выбора, обоснования, реализации и контроля результатов управленческого решения.		
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам	Этапы: - выполнение производственных эксплуатационных работ, - оформления отчёта 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 саморазви-		ФОС: Текст доклада и презентация

	тия, самостоятельного приобретения и освоения новых знаний - навыками критической оценки своих достоинств и недостатков - опытом выбора средств и возможностей развития достоинств и устранения недостатков		по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике
ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать - виды информационного взаимодействия и обслуживания; - аппаратные средства вычислительной техники; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации; - основные задачи, понятия, математические методы и алгоритмы криптографии.	Этапы: - выполнение производственных эксплуатационных работ, - оформления отчёта по результатам самостоятельной работы по теме практики	ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседование на защите отчета по практике
	Уметь - 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.		
	Владеть навыками безопасного использования технических средств в профессиональной деятельности.		
ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информа-	Знать - принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); - защитные механизмы и средства обеспечения сетевой безопасности;	Этап - этап выполнения производственных эксплуатационных работ	ФОС: Текст отчета, устный доклад и презентация по результатам самостоятельной работы по теме практики

ционной безопасности объекта защиты	- защита в операционных системах; - средства и методы предотвращения и обнаружения вторжений; - способы и средства защиты информации от утечки по техническим каналам		
	Уметь - формулировать и настраивать политику безопасности основных ОС, а так же локальных компьютерных сетей, построенных на их основе; - использовать средства защиты, представляемые СУБД; - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях		ФОС: Практическое задание. Собеседование на защите отчета по практике
	Владеть - навыками конфигурирования и администрирования ОС; - методиками анализа системного трафика; - методиками анализа результатов работы средств обнаружения вторжений; - навыками настройки межсетевых экранов		Отзыв руководителя практики от предприятия. ФОС: Собеседование на защите отчета по практике
ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знать - методы и средства контроля эффективности технической защиты информации	Этапы: - выполнение производственных эксплуатационных работ, - оформления отчёта по результатам самостоятельной работы по теме практики	ФОС: Собеседование на защите отчета по практике. Текст отчета, устный доклад и презентация по результатам самостоятельной работы по теме практики. Отзыв руководителя практики от предприятия
	Уметь - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем		
	Владеть - навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; - навыками участия в экс-		

	пертизе состояния защищенности информации на объекте защиты.		

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 10. 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 единицы, 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 исследова-

ния; 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 коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
- способность к самоорганизации и самообразованию (ОК-8);

Профессиональные компетенции (ПК):

- способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);
- способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
- способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);
- способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

Формы промежуточной аттестации (по итогам практики)

Зачет с оценкой.

Фонд оценочных средств для проведения промежуточной аттестации по практике

Таблица 11. 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 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	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: 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. 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-x.

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 информацион-

	ных 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 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	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 Ж, З).

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.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 (темы) дисциплины или модуля и их наименование)	Форма отчетности практиканта, ФОС* (средства оценивания)
ОК-7 способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	Знать - свойства русского языка как средства общения и передачи информации, грамматику, культуру и традиции стран изучения иностранного языка,	Этапы: – научно-исследовательский, - оформления отчёта	ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике.
	Уметь - целесообразно использовать знание русского языка, культуры речи и навыков общения в профессиональной деятельности - проводить сбор, обработку, анализ и систематизацию научно-технической информации.		
	Владеть - навыками работы с технической документацией.		
ОК-8 способность к самоорганизации и самообразованию	Знать - основные методы обработки и анализа научно-технической информации по исследуемым проблемам и задачам	Этапы: – научно-исследовательский, - выполнения самостоятельных работ по теме практики, - оформления отчёта	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		ФОС: Текст доклада и презентация по результатам самостоятельной работы на практике. Собеседо-

	- навыками критической оценки своих достоинств и недостатков - опытом выбора средств и возможностей развития достоинств и устранения недостатков		вание на защите отчета по практике
ПК-7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	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: – научно-исследовательский, - выполнения самостоятельных работ по теме практики, - оформления отчёта	ФОС: Собеседование по вопросам ФОС для курса Основы информационной безопасности и вопросам из Приложения Ж.
	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		ФОС: Собеседование, анализ выполнения практического задание
	Владеть -методами управления информационной безопасностью информационных систем; - методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение эксперименталь-		ФОС: Текст доклада и презентация по результатам самостоятельной работы по теме практики

	ных исследований системы защиты информации; - методами оценки информационных рисков		
ПК-8 способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации	Этап – оформления отчёта по итогам практики	ФОС: Текст доклада и презентация по результатам самостоятельной работы по теме практики
	Уметь - пользоваться нормативными документами по защите информации; - пользоваться методиками проверки защищенности объекта информатизации		
	Владеть - навыками работы с нормативными правовыми актами по технической защите информации		
ПК-9 способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации	Этапы: – научно-исследовательский, - выполнения 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		ФОС: Собеседование на защите отчета по практике
	Владеть - навыками работы с нормативными правовыми актами в области ИБ; - навыками работы с нормативными правовы-		ФОС: Ответы на вопросы на защите отчета по практике Отзыв руководителя практики

	ми актами по технической защите информации		
ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать - основы организационного и правового обеспечения информационной безопасности; - основные нормативные правовые акты в области информационной безопасности и защиты информации	Этапы: – научно-исследовательский, - выполнения самостоятельных работ по теме практики, - оформления отчёта	ФОС: Практическое задание, текст доклада и презентация по результатам самостоятельной работы по теме практики
	Уметь - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем		
	Владеть Навыками применения методик проверки защищенности объекта информатизации		
ПК-12 способность принимать участие в проведении экспериментальных исследований системы защиты информации	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: - выполнения 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		
	Владеть - методами управления информационной безопасностью информаци-		

	онных систем; - методами оценки информационных рисков		

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

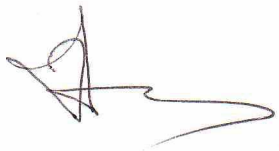
Для дескрипторов категорий «Уметь» и «Владеть»:

- 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.

ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ  Э.К. Алгазинов

Приложение А
(обязательное)

Форма отзыва руководителя от предприятия

Реквизиты предприятия

_____ № _____
дата отзыва *исх. № документа*

О Т З Ы В

о прохождении производственной практики
обучающимся __ курса __ группы
факультета компьютерных наук

_____
И.О. Фамилия

Обучающийся _____ проходил(а) производственную практику
И.О. Фамилия
на базе _____ в период с __.__.20__ по __.__.20__
наименование предприятия
В процессе прохождения практики обучающимся выполнялись работы и задания по теме

_____
название темы

_____
(Характеристика выполняемых работ,

_____
перечисление достоинств и недостатков работы)

_____

_____

_____

Считаю, что с учетом перечисленных достоинств и недостатков работа заслуживает оценки _____.
оценка по четырех балльной шкале

Руководитель практики от предприятия _____
_____
Подпись *расшифровка подпси*

Руководитель предприятия _____ _____
Подпись *расшифровка подписи*

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>

Направление 10.03.01 Информационная безопасность

Профиль «Безопасность 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 персональных 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 Д
(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.2 Учебная практика практике 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 я 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 Е
(рекомендуемое)

Список вопросов для проведения собеседования
по учебной технологической 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 технологической практике

Б2.У.3 Учебная технологическая 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 Ж
(рекомендуемое)

Список вопросов для проведения собеседования по производственной проектно-технологической 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 производственной проектно-технологической практике

Б2.П.1 Производственная проектно-технологическая практика

Примерный список заданий для студентов по производственной проектно-технологической 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 проектно-технологической 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 3
(рекомендуемое)

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

Б2.П.2 Производственная 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.