

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: и.о. декана факультета фундаментальной и прикладной информатики
Дата подписания: 06.10.2022 12:59:21
Уникальный программный ключ:
65ab2aa0d384efe8480e6a4c688eddbc475e411a

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

фундаментальной и прикладной

(наименование ф-та полностью)

информатики



М.О. Таныгин

(подпись, инициалы, фамилия)

« 30 » *QR* 2021 г

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

(наименование вида практики)

Технологическая практика

(наименование типа практики)

направление подготовки (специальность)

10.05.02

(шифр согласно ФГОС)

Информационная безопасность телекоммуникационных систем

и наименование направление подготовки (специальности)

Защита информации в системах связи и управления

наименование профиля, специализации или магистерской программы

форма обучения

очная

(очная, очно-заочная, заочная)

Программа составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», утвержденным приказом Министерства образования и науки РФ от 16.11.2016 г. №1426 и на основании учебного плана специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», специализация "Защита информации в системах связи и управления", одобренным Ученым советом университета (протокол №5 «30» января 2017 г.).

Программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» на заседании кафедры информационной безопасности.

«28» августа 2017 г. Протокол № 1

И.о. зав. кафедрой ИБ

Таныгин М.О.

Разработчик программы
доцент кафедры ИБ, к.т.н.

Таныгин М.О.

Директор научной библиотеки

Макаровская В.Г.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности, протокол №12 от 29.06.18 г.

Зав. кафедрой

Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности, протокол №11, от 27.06.2018 г.

Зав. кафедрой

Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности, протокол №1, от 31.08.2020 г.

Зав. кафедрой

Таныгин М.О.

1 Цель и задачи практики. Вид, тип, способ и форма (-ы) ее проведения

1.1. Цель практики

Целью технологической практики является обеспечение тесной связи между научно-теоретической и практической подготовкой специалистов, развитие профессиональных навыков и умений в области обеспечения информационной безопасности.

1.2. Задачи практики

1. Формирование общекультурных и профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за практикой по получению профессиональных умений и опыта профессиональной деятельности.

2. Освоение современных информационных технологий и профессиональных программных комплексов, применяемых в области информационной безопасности.

3. Совершенствование навыков подготовки, представления и защиты информационных, аналитических и отчетных документов по результатам профессиональной деятельности и практики.

4. Развитие исполнительских и лидерских навыков обучающихся.

1.3 Вид, тип, способ и форма (-ы) ее проведения

Вид практики – производственная.

Тип практики – технологическая.

Способ проведения практики – стационарная (в г. Курске) и выездная (за пределами г. Курска). ФГОС ВО разрешает оба способа проведения данной практики, поэтому способ ее проведения устанавливается конкретно для каждого обучающего в зависимости от места расположения предприятия, организации, учреждения, в котором он проходит практику.

Практика проводится на предприятиях, в организациях и учреждениях, с которыми университетом заключены соответствующие договоры.

Практика проводится на предприятиях различных отраслей и форм собственности, в органах государственной или муниципальной власти, академических или ведомственных научно-исследовательских организациях, учреждениях системы высшего или дополнительного профессионального образования, деятельность которых связана с вопросами информационной безопасности и соответствует профессиональным компетенциям, осваиваемым в рамках образовательной программы: в ФОИВ РФ, ФОИВ субъектов РФ и муниципальных образований, на кафедрах информационной безопасности, обладающих необходимым кадровым и научно-техническим потенциалом, и т.п.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики, представленному в разделе 4 настоящей программы.

Выбор мест прохождения практики для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

*Форма проведения практики** Производственная (технологическая) практика проходит непрерывно в 11 семестре на 6 курсе, продолжительность - 4 недели.

2 Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (компетенции)		Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)
Код компетенции	Содержание компетенции	
ПК-8	способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем	Знать: Принципы построения технических и программно-аппаратных средств защиты телекоммуникационных систем.
		Уметь: Проводить тестирование технических и программно-аппаратных средств защиты.
		Владеть: Навыками анализа эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем.
ПК-9	способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации	Знать: Техническое обслуживание оборудования защищенных телекоммуникационных сетей.
		Уметь: Формулировать технические требования к телекоммуникационным системам и нормам.
		Владеть: Навыками проведения аттестации телекоммуникационных сетей.
ПК-10	способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений	Знать: Инструментальные средства обеспечения защиты информации телекоммуникационных систем.
		Уметь: Формулировать технические требования нормативных правовых актов к телекоммуникационным системам и нормам.
		Владеть: Навыками эксплуатации телекоммуникационных приборов и средств защиты информации.
ПСК-10.4	способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации	Знать: Защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений, перехвата информации. Уметь: Применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для за-

Планируемые результаты освоения образовательной программы (компетенции)		Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)
Код компетенции	Содержание компетенции	
		щиты информации и закрытия возможных каналов ее перехвата в беспроводных сетях передачи данных. Владеть: Навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов.

3 Место практики в структуре образовательной программы. Объем практики в зачетных единицах и ее продолжительности в неделях либо в академических или астрономических часах

В соответствии с учебным планом производственная (технологическая) практика (Б2.П.4) входит в блок Б2 «Практики, в том числе научно-исследовательская работа».

Практика является обязательным разделом образовательной программы и представляет собой вид учебных занятий, направленный на формирование, закрепление, развитие практических умений, навыков и компетенций в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью. Практика тесно связана с ранее изученными дисциплинами и направлена на обеспечение непрерывности и последовательности овладения обучающимися видами профессиональной деятельности, установленными образовательной программой.

Технологическая практика по проводится на 6-м курсе в 11-м семестре.

Объем технологической практики, установленный учебным планом, – 6 зачетных единиц, продолжительность – 4 недели (216 часов).

4 Содержание практики

Содержание практики уточняется для каждого обучающегося в зависимости от специфики конкретного предприятия, организации, учреждения, являющегося местом ее проведения, и выдается в форме задания на практику.

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практи-	6

		ки; 3) получение заданий от руководителя практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	
2	Подготовительный этап (работа на предприятии)	Решение организационных вопросов на предприятии: 1) Знакомство с предприятием, с внутренним распорядком предприятия, руководителем практики от предприятия, рабочим местом и должностной инструкцией. 2) Проведение инструктажей по технике безопасности на рабочем месте, противопожарной профилактике. 3) получение задания от руководителя практики от предприятия.	10
3	Основной этап (работа на предприятии)	Изучение нормативных документов, регулирующих работу, относящуюся к должностным обязанностям (положения, приказы, инструкции, памятки и др.) Выполнение индивидуального задания на практику	156
4	Заключительный этап	Оформление дневника практики. Составление отчета о практике. Представление дневника практики и защита отчета о практике на промежуточной аттестации.	44

Технологическая практика должна включать в себя в обязательном порядке следующие мероприятия:

- получение теоретических знаний;
- практическую работу.

Для прохождения практики каждому студенту выдается:

- индивидуальное задание;

Индивидуальное задание включает техническое задание, которое выполняется студентами самостоятельно. Содержание индивидуального задания может быть связано с темами выпускных квалификационных работ магистров.

5 Формы отчетности по практике

Формы отчетности студентов о прохождении производственной (технологической) практики:

- дневник практики

(https://www.swsu.ru/structura/umu/training_division/blanks.php),

- отчет о практике.

Структура отчета о технологической практике:

- 1) Титульный лист.
- 2) Содержание.
- 3) Введение. Цель и задачи практики. Общие сведения о предприятии, организации, учреждении, на котором проходила практика.
- 4) Основная часть отчета.
- 5) Заключение. Выводы о достижении цели и выполнении задач практики.
- 6) Список использованной литературы и источников.
- 7) Приложения (иллюстрации, таблицы, карты и т.п.).

Отчет должен быть оформлен в соответствии с:

- ГОСТ Р 7.0.12-2011 Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила.

- ГОСТ 2.316-2008 Единая система конструкторской документации. Правила нанесения надписей, технических требований и таблиц на графических документах. Общие положения;

- ГОСТ 7.32-2001 Отчет о научно-исследовательской работе. Структура и правила оформления;

- ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам;

- ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Общие требования и правила составления;

- ГОСТ 2.301-68 Единая система конструкторской документации. Форматы;

- ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления;

- ГОСТ 7.9-95 (ИСО 214-76). Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация. Общие требования.

-СТУ 04.02.030-2015 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению»

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-8 - способность проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем	Техническая защита информации Программно-аппаратные средства обеспечения информационной безопасности		Комплексное обеспечение информационной безопасности инфокоммуникационных систем Технологическая практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-9 - способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации	Измерения в телекоммуникационных системах		Планирование и управление информационной безопасностью Основы мониторинга безопасности инфокоммуникационных систем и сетей Система сертификации и аттестации телекоммуникационных систем Порядок проведения аттестации объектов информатизации Технологическая практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-10 - способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений	Система сертификации и аттестации телекоммуникационных систем Порядок проведения аттестации объектов информатизации Технологическая практика Преддипломная практика		Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПСК-10.4 - способность	Техническая защита информации		Комплексное обеспечение информационной безопасности инфокоммуникационных си-

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации			<p>STEM</p> <p>Технологическая практика</p> <p>Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты</p>

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции/ этап (указывается название этапа из п.6.1)	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-8/ завершающий	<p>1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики</p> <p>2. Качество освоенных обучающимся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.</p>	<p>Знает: Поверхностно понятие и принципы телекоммуникационных систем.</p> <p>Умеет: пользоваться существующей документацией и на ее примере разрабатывать новую.</p> <p>Владеет: слабо владеет навыками решения стандартных задач в профессиональной деятельности по обеспечению заданного уровня безопасности телекоммуникационных систем.</p>	<p>Знает: Углубленно, но с некоторыми пробелами в отдельных областях построения технических и программно-аппаратных средств.</p> <p>Умеет: в достаточной мере проводить на практике современные методы тестирования технических средств защиты.</p> <p>Владеет: Навыками решения стандартных задач в профессиональной деятельности по обеспечению заданного уровня безопасности телекоммуникационных систем.</p>	<p>Знает: Углубленно принципы построения технических и программно-аппаратных средств защиты телекоммуникационных систем.</p> <p>Умеет: успешно проводить тестирование технических и программно-аппаратных средств защиты.</p> <p>Владеет: Навыками анализа эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем.</p>
ПК-9/	1. Доля осво-	Знает:	Знает:	Знает:

Код компетенции/ этап (указываются название этапа из п.6.1)	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо)	Высокий уровень («отлично»)
1	2	3	4	5
завершающий	<p>енных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p> <p>3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>С пробелами основное техническое оборудование защищенных телекоммуникационных сетей.</p> <p>Умеет: в недостаточной форме формулировать технические требования средств защиты информации в телекоммуникационных системах.</p> <p>Владеет: слабо владеет навыками решения профессиональных задач.</p>	<p>Углубленно, но с некоторыми пробелами в отдельных областях технические возможности информационной безопасности телекоммуникационных систем.</p> <p>Умеет: в достаточной мере формулировать технические требования средств защиты информации в телекоммуникационных системах.</p> <p>Владеет: навыками программирования в профессиональной сфере.</p>	<p>Углубленно техническое обслуживание оборудования защищенных телекоммуникационных сетей.</p> <p>Умеет: успешно формулировать технические требования к телекоммуникационным системам и нормам.</p> <p>Владеет: развитыми навыками проведения аттестации телекоммуникационных сетей.</p>
ПК-10 /завершающий	<p>1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p>	<p>Знает: Основные правила организации защиты информации телекоммуникационных систем.</p> <p>Умеет: В недостаточной форме находить правильные нормативные правовые акты к телекоммуникационным системам и нормам.</p> <p>Владеет: Навыками организации работы отдельных телекоммуникационных приборов.</p>	<p>Знает: Основные принципы обеспечения защиты информации телекоммуникационных систем.</p> <p>Умеет: Осуществлять выбор технические требования нормативных правовых актов к телекоммуникационным системам и нормам.</p> <p>Владеет: Навыками использования телекоммуникационных приборов.</p>	<p>Знает: Глубокие знания в области эксплуатации телекоммуникационных приборов и средств защиты информации.</p> <p>Умеет: Формулировать технические требования нормативных правовых актов к телекоммуникационным системам и нормам.</p> <p>Владеет: Умелыми навыками эксплуатации инструментальных средств обеспечения</p>

Код компетенции/ этап (указывается название этапа из п.6.1)	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо)	Высокий уровень («отлично»)
1	2	3	4	5
	3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.			защиты информации телекоммуникационных систем.
ПСК-10.4 /завершающий	<p>1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики</p> <p>2. Качество освоенных обучающимся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.</p>	<p>Знает: имеет представление об основных средствах и методах предотвращения и обнаружения вторжений, перехвата информации.</p> <p>Умеет: имеет представление о применении на практике основных средства защиты информации и закрытия возможных каналов ее перехвата акустической речевой информации в беспроводных сетях передачи данных.</p> <p>Владеет: в общих понятиях владеет навыками конфигурирования локальных сетей, настройки межсетевых экранов.</p>	<p>Знает: основные средства и методы предотвращения и обнаружения вторжений, перехвата информации.</p> <p>Умеет: применять на практике основные средства защиты информации и закрытия возможных каналов перехвата акустической речевой информации в беспроводных сетях передачи данных.</p> <p>Владеет: навыками управления локальной сетью, реализации сетевых протоколов с помощью программных средств.</p>	<p>Знает: особенности применения защитных механизмов и средств обеспечения сетевой безопасности, свободно ориентируется в применении средств и методов предотвращения и обнаружения вторжений, перехвата информации.</p> <p>Умеет: применять защищенные протоколы, конфигурировать межсетевые экраны и средства обнаружения вторжений для защиты информации и закрытия возможных каналов ее перехвата в беспроводных сетях передачи данных.</p> <p>Владеет: навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов.</p>

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Код компетенции/этап формирования компетенции в процессе освоения ОП ВО (указывается название этапа из п.6.1)	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности
1	2
ПК-8/ завершающий	Дневник практики. Характеристика руководителя практики от предприятия лидерских качеств обучающегося.
ПК-9 / завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике).
ПК-10/ завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПСК-10.4 /завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Ответы на вопросы по содержанию практики на промежуточной аттестации.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной (технологической) практикой, осуществляется в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение практики на месте ее проведения руководителем практики от предприятия.

Промежуточная аттестация проводится в 11-м семестре в форме зачета с оценкой. На зачет обучающийся представляет дневник практики и отчет о практике. Зачет проводится в форме устной защиты отчета о практике.

Таблица 6.4.1 – Шкала оценки отчета о практике и его защиты

№	Предмет оценки	Критерии оценки	Максимальный балл
---	----------------	-----------------	-------------------

1	Содержание отчета 10 баллов	Достижение цели и выполнение задач практики в полном объеме	1
		Отражение в отчете всех предусмотренных программой практики видов и форм профессиональной деятельности	1
		Владение актуальными нормативными правовыми документами и профессиональной терминологией	1
		Соответствие структуры и содержания отчета требованиям, установленным в п. 5 настоящей программы	1
		Полнота и глубина раскрытия содержания разделов отчета	1
		Достоверность и достаточность приведенных в отчете данных	1
		Правильность выполнения расчетов и измерений	1
		Глубина анализа данных	1
		Обоснованность выводов и рекомендаций	1
		Самостоятельность при подготовке отчета	1
2	Оформление отчета 2 балла	Соответствие оформления отчета требованиям, установленным в п.5 настоящей программы	1
		Достаточность использованных источников	1
3	Содержание и оформление презентации (графического материала) 4 балла	Полнота и соответствие содержания презентации (графического материала) содержанию отчета	2
		Грамотность речи и правильность использования профессиональной терминологии	2
4	Ответы на вопросы о содержании практики 4 балла	Полнота, точность, аргументированность ответов	4

Баллы, полученные обучающимся, суммируются, соотносятся с уровнем сформированности компетенций и затем переводятся в традиционные оценки.

Таблица 6.4.2 – Соответствие баллов уровням сформированности компетенций и традиционным оценкам

Баллы	Уровень сформированности компетенций	Оценка
18-20	высокий	отлично
14-17	продвинутый	хорошо
10-13	пороговый	удовлетворительно
9 и менее	недостаточный	неудовлетворительно

7 Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

7.1 Основная литература:

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

2. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический уни-

верситет. - СПб.: Издательство Политехнического университета, 2014. - 322 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=363040>

3. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие / В. А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=440285>

4. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Форум, 2004. - 154 с.

7.2 Дополнительная литература:

1) Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Режим доступа:

<http://biblioclub.ru/index.php?page=book&id=93245>

2) Абрамов, Г. В. Проектирование информационных систем [Электронный ресурс] : учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=141626>

3) Дреус, Ю. Г. Организация ЭВМ и вычислительных систем [Текст] : учебник / Ю. Г. Дреус. - М. : Высшая школа, 2006. - 501 с.

4) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=276557>

5) Куль, Т. П. Операционные системы [Электронный ресурс] : учебное пособие / Т. П. Куль. - Минск : РИПО, 2015. - 312 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=463629>

6) Курячий, Г. В. Операционная система UNIX [Электронный ресурс] : методические рекомендации / Г. В. Курячий. - М. : Интернет-Университет Информационных Технологий, 2004. - 288 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=233108>

7) Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

8) Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с.

9) Олифер, В. Г. Сетевые операционные системы [Текст] : учебное пособие / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2003. - 539 с.

10) Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие / В. И. Петренко ; Министерство образования и науки

Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. -Режим доступа : <http://biblioclub.ru/index.php?page=book&id=458204>

11) Ярочкин, В. И. Безопасность информационных систем [Текст] /В. И. Ярочкин. - М. : Ось-89, 1996. - 320 с.

7.3 Перечень методических указаний

1) Практика. [Электронный ресурс]: методические указания по написанию отчета и защиты практики для студентов всех форм обучения направления подготовки (специальности) 10.00.00 Информационная безопасность/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, И.В. Калуцкий – Электрон. текстовые дан. - Курск, 2018. – 40 с.: прилож.5. – Библиогр.: 21 стр.

2) Научно-исследовательская работа студентов. [Электронный ресурс]: методические рекомендации по проведению, содержанию, оформлению и защите отчета НИРС для студентов всех форм обучения направления подготовки (специальности), 10.00.00 Информационная безопасность/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, А.Л. Марухленко – Электрон. текстовые дан. - Курск, 2018. – 27 с.: прилож.4. – Библиогр.: 22 стр.

7.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет

- 1) Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>
- 2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>
- 3) Сообщество Ubuntu [официальный сайт]. Режим доступа: <http://ubuntu.com/>
- 4) Корпорация Microsoft [официальный сайт]. Режим доступа: <http://microsoft.com/>
- 5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: <http://biblioclub.ru>
- 6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: <http://www.consultant.ru>
- 7) Научно-информационный портал ВИНТИ РАН [официальный сайт]. Режим доступа: <http://www.consultant.ru/>
- 8) База данных "Патенты России"

8 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- 1) Microsoft Office 2016. Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;
- 2) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,
- 3) Windows 7, договор IT000012385;
- 4) Oracle Virtualbox (Бесплатная, GNU General Public License);
- 5) редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО <http://www.hhdssoftware.com/free-hex-editor/>);
- 6) открытая среда разработки программного обеспечения Lazarus (Свободное ПО <http://www.lazarus.freepascal.org/>);
- 7) ОС FreeBSD (свободное ПО, лицензия BSD), ОС Ubuntu (Бесплатная, GNU GPLv3);
- 8) GNS3 - графический симулятор сети (свободное ПО).

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется оборудование конкретного предприятия (организации, учреждения), на базе которого она проводится. Отделы и лаборатории предприятия (организации, учреждения) должны соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.:

– Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (12 шт) Компьютер NORBEL C239264Ц-AMD/2x8Gb/2TB/DVDRW/LCD 20";

- МФУ Canon iR 2520
- Межсетевой экран Netgear STM150EW-100EUS
- Роутер ASUS WL-520GC
- Маршрутизатор D-Link DFL-860E
- Коммутатор TrendNet TE100-S88E + 8 port 10/100 Switch
- Система виброакустического шумления «Шорох-2», виброакустический датчик КПВ-2, акустический излучатель OMS -2000
- Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”
- Комбинированный поисковый прибор “D008”
- Универсальный поисковый прибор "СРМ-700"
- Лазерный дальномер Mettler 60
- Генератор шума Соната-С1

Для проведения промежуточной аттестации по практике необходимо следующее материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24