МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Василенко В.Н.

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели и задачи практики

Целями производственной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте.

Задачи :

– углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;

– усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

– развитие навыков администрирования подсистем информационной безопасности.

Объектами профессиональной деятельности специалистов являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно- технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

2. Перечень планируемых результатов обучения при прохождении практики

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

– способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

– способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

– способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

– способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

– способностью осуществлять поиск, изучение, обобщение и систематизацию научно- технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

– способностью создавать и исследовать модели автоматизированных систем (ПК-2);

– способностью проводить анализ защищенности автоматизированных систем (ПК-3);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способностью разрабатывать научно-техническую документацию, готовить научно- технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

– способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

– способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

– способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК- 14);

– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

– способностью управлять информационной безопасностью автоматизированной системы (ПК-28);

– способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);

– способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);

– способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);

– способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);

– способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).

В результате прохождения практики обучающийся должен:

Знать:

– основные понятия и задачи векторной алгебры и аналитической геометрии (ОПК-1);

– современные технологии и методы программирования (ОПК-3);

– формы и способы представления данных в персональном компьютере (ОПК-4);

– методы научных исследований в профессиональной деятельности (ОПК-5);

– основы организационного и правового обеспечения информационной безопасности (ОПК-6);

– технику безопасности при работе с приборами и оборудованием для защиты информации (ОПК-7);

– основные технические и программные средства защиты информации, используемые на предприятии (ОПК-8);

– предъявляемые в организациях требования к специалистам, работающим в области защиты информации (ПК-1);

– основные технологии защиты информации, используемые на предприятии (ПК-2);

– средства обеспечения безопасности данных (ПК-3);

– источники и классификацию угроз информационной безопасности (ПК-4);

– основные риски информационной безопасности (ПК-5);

– мировые и российские стандарты в области информационной безопасности (ПК-6);

– принципы организации документирования разработки, процесса сопровождения программного обеспечения (ПК-7);

– характеристики каналов передачи данных (ПК-10);

– принципы построения систем защиты информации (ПК-11);

– компоненты системы управления информационной безопасностью автоматизированной системы (ПК-12);

– методы и средства проектирования средств защиты информации (ПК-13);

– процесс сопровождения программного обеспечения (ПК-14);

– правовые акты по аттестации объектов информатизации и сертификации средств защиты информации (ПК-15);

– нормативную документацию в области аттестации автоматизированных систем (ПК-16);

– функции межсетевых экранов, профили защиты для межсетевых экранов (ПК-17);

– методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем (ПК-20);

– разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– задачи систем анализа защищенности в защите открытых систем (ПК-22);

– состав информации ограниченного доступа организации (ПК-23);

– слабости системных утилит, команд и сетевых сервисов (ПК-24);

– методы, принципы, процедуры и службы администрирования информационных систем (ПК-26);

– основные протоколы компьютерных сетей (ПК-27);

– технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования (ПК-28);

– комплексном подходе к построению эшелонированной защиты для автоматизированных систем (ПСК-4.1);

– понятия информационной безопасности, защиты информации, назначение и основные возможности систем защиты информации (ПСК-4.2);

– основные компоненты архитектуры мобильных платформ (ПСК-4.3);

– терминологию и системный подход построения защищенных открытых информационных систем (ПСК-4.4);

– принципы декодирования HTTP (ПСК-4.5).

Уметь:

– определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач (ОПК-1);

– применять при решении профессиональных задач с использованием вычислительной техники соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации (ОПК-2);

– строить логические и правильные программы (ОПК-3);

– применять средства восстановления системы после сбоя, чистки и дефрагментации диска (ОПК-4);

– проводить комплексное проектировать структуру и архитектуру программного обеспечения с использованием современных методологий (ОПК-5);

– применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ОПК-6);

– работать с офисной техникой и специализированным оборудованием с учетом требований техники безопасности (ОПК-7);

– пользоваться приборами выявления каналов утечки информации, обнаружения подслушивающих устройств и приборов незаконного съема информации, локализации действия средств несанкционированного доступа (ОПК-8);

– работать со специализированными прикладными программами, инструментальной системой программирования и ресурсами Интернет (ПК-1);

– применять основные законы и нормативные документы в области информационной безопасности (ПК-3);

– проводить мониторинг угроз безопасности компьютерных сетей (ПК-4);

– планировать политику безопасности операционных систем (ПК-5);

– применять на практике методы анализа электрических цепей (ПК-6);

– пользоваться нормативными документами но противодействию технической

разведке (ПК-7);

– проводить анализ проектных решений по обеспечению информационной безопасности (ПК-8);

– формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения (ПК-9);

– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей (ПК- 10);

– участвовать в разработке политики информационной безопасности (ПК-11);

– проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов (ПК-13);

– участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств (ПК-14);

– участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15);

– соблюдать правила вежливости и культуры поведения в профессиональной деятельности давать нравственную оценку коррупционным проявлениям и другим нарушениям норм профессиональной этики (ПК-18);

– участвовать в разработке предложений по совершенствованию системы управления информационной безопасностью (ПК-19);

– участвовать в коллективной разработке проектов документов по обеспечению информационной безопасности (ПК-21);

– применять принципы формирования политики информационной безопасности (ПК-22);

– применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем (ПК-23);

– применять математические методы при решении профессиональных задач моделирования повышенной сложности (ПК-24);

– использовать частные и обобщенные модели систем комплексной защиты информации (ПК-25);

– участвовать в администрировании подсистемы информационной безопасности (ПК-26);

– разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных (ПК-27);

– участвовать в работе коллектива по управлению информационной безопасностью организации (ПК-28);

– открывать и закрывать общий доступ к информации в локальной сети (ПСК-4.2);

– устранять источники угроз безопасности мобильных систем и приложений (ПСК-4.3);

– проектировать взаимодействия многомашинных информационных систем, используя стандартные протоколы эталонной модели (ПСК-4.4);

– создавать CGI, ISAPI и WEB приложения (ПСК-4.5).

Владеть:

– навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач (ОПК-1);

– расчетными формулами, компьютерными программами при решении математических задач (ОПК-2);

– составления программ по разработанным алгоритмам (ОПК-3);

– навыками работы с современными информационными технологиями для поиска информации (ОПК-4);

– навыками организации и обеспечения режима секретности (ОПК-6);

– навыками работы с измерительными приборами и типовым оборудованием для

защиты информации (ОПК-7);

– методиками проведения аналитической работы по предупреждению утечки конфиденциальной информации (ОПК-8);

– применения руководящих и нормативных документов по инженерно-технической защите информации (ПК-1);

– навыками проектирования программного обеспечения с использованием средств автоматизации (ПК-2);

– навыками анализа основных узлов устройств современных автоматизированных систем (ПК-3);

– навыками программирования в профессиональной деятельности (ПК-4);

– навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем (ПК-5);

– навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств (ПК-6);

– навыками разработки, документирования, тестирования и отладки программного обеспечения (ПК-7);

– профессиональной терминологией в области информационной безопасности (ПК-8);

– способностью учувствовать в разработке защищенных автоматизированных систем (ПК-9);

– планирования политики безопасности операционных систем (ПК-11);

– навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей (ПК-12);

– навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15);

– навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры (ПК-16);

– выбора и использования архитектурных особенностей вычислительных систем различных классов (ПК-17);

– навыками конструктивного общения в процессе профессиональной деятельности (ПК-18);

– методами формирования требований по защите информации (ПК-19);

– навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– навыками работы с сетевыми сканерами, сканерами безопасности (ПК-25);

– средствами SQL Server для администрирования удаленных баз данных (ПК-26);

– навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия (ПСК-4.1);

– навыками программирования простейших методов шифрования-дешифрования (ПСК- 4.3);

– навыками оценивания стойкости различных паролей (ПСК-4.4);

– навыками формирования ключей шифрования с заданной стойкостью (ПСК-4.5).

3. Место практики в структуре ООП

Производственная практика (по получению профессиональных умений и опыта профессиональной деятельности) относится к базовой части Блока 2 «Практики» образовательной программы.

Практика является важнейшей составной частью учебного процесса подготовки специалистов и проводится на основании учебного плана по направлению 10.05.03 – Информационная безопасность автоматизированных систем, в соответствии с требованиями Федерального Государственного образовательного стандарта высшего образования.

Для успешного прохождения практики необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Экология», «Программно-аппаратные средства обеспечения информационной безопасности», «Организационно-правовое обеспечения информационной безопасности», «Защита web-сайтов», «Учебная практика (по получению первичных профессиональных умений и навыков научно-исследовательской деятельности)».

Для освоения производственной практики студент должен:

- знать законодательные и нормативные нормы и регламенты организации работы с персоналом по защите персональных данных;
- уметь применять технические и программные средства защиты информации;
- владеть информационными технологиями защиты информации на предприятии.

Знания, умения и навыки, сформированные при прохождении практики, необходимы для успешного освоения последующих дисциплин «Преддипломная практика», «Защита конфиденциальной информации», «Надежность информационных систем».

4. Место и время проведения практики

Практика проводится в 8 семестре.

Практика проводится в организации, осуществляющей деятельность по направленности (профилю) образовательной программы (далее – профильная организация), и (или) непосредственно в структурном подразделении ФГБОУ ВО «ВГУИТ» (далее – ВГУИТ).

Для лиц с ограниченными возможностями здоровья и инвалидов место прохождения практики учитывает особенности их психофизического развития,

Практика является стационарной и выездной, и может проводиться в отделах защиты информации, отделах АСУ, вычислительных центрах, отделах, занимающихся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей, отделах, занимающихся разработкой, продвижением и поддержкой web-сайтов.

5. Структура и содержание практики

Общая трудоемкость прохождения практики составляет 3 зачетных единицы; 108 академических часов, 2 недели. Контактная работа обучающегося (КРо) составляет 72 ч. Иные формы работы 36 ч.

№ п/п	Разделы (этапы) практики	Трудоемкость, акад. ч	
		Контактная работа	Иные формы работы
1	**Подготовительный этап**	**4**	**-**
1.1	Инструктаж по программе практики, подготовке отчета и процедуре защиты	2	
1.2	Инструктаж по технике безопасности по месту прохождения практики	2	
2	**Рабочий этап**		
2.1	Работа с источниками и поиск информации	8	
2.2	Аналитический обзор нормативно-правовой документации предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения, на котором проводится практика; описание видов, методов, средств информационной защиты, применяемых на предприятии;	20	
2.3	Выполнение установки, настройки или эксплуатации компонентов системы обеспечения информационной	20	

	безопасности согласно индивидуальным задачам производственной практики		
3	**Отчетный этап**		
3.1	Подготовка отчета к защите, публикации по теме практической подготовки	10	18
3.2	Промежуточная аттестация по практике	10	18
	Итого за В семестр	**72**	**36**
	Всего:	**72**	**36**

6. Формы промежуточной аттестации (отчётности по итогам практики)

Отчет и дневник практик необходимо составлять во время практики по мере обработки того или иного раздела программы. По окончании практики и после проверки отчета руководителями практики от производства и кафедры, студент защищает отчет в установленный срок перед комиссией, назначаемой заведующим кафедрой.

По окончании срока практики, руководители практики от Университета доводят до сведения обучающихся график защиты отчетов по практике.

В течение двух рабочих дней после окончания срока практики обучающийся предоставляет на кафедру отчет и дневник по практике, оформленные в соответствии с требованиями, установленными программой практики с характеристикой работы обучающегося, оценками прохождения практики и качества компетенций, приобретенных им в результате прохождения практики, данной руководителем практики от организации.

В двухнедельный срок после начала занятий обучающиеся обязаны защитить его на кафедральной комиссии, график работы которой доводится до сведения студентов.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и характеристики руководителя практики от организации. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно). **Отчет и дневник** по практике обучающийся сдает руководителю практики от Университета.

7. Оценочные материалы для промежуточной аттестации обучающихся по практике

7.1. Оценочные материалы (ОМ) для практики включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

– описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

– 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;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

7.2. Для каждого результата обучения по практике определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

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

8.1. Учебные печатные и электронные издания

Материалы, полученные во время прохождения практики.

При выполнении программы практики студент может использовать учебно-методическое и информационное обеспечение дисциплин учебного плана, предшествующих выполнению программы практики.

Кроме того, необходимо использовать материалы профессиональных периодических изданий и иные информационные ресурсы.

1. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В.

Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428820. – Текст : электронный.

2. Системы защиты информации в ведущих зарубежных странах : учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. : ил., схем. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93351. – Текст : электронный.

3. Костин, В. Н. Методы и средства защиты компьютерной информации: криптографические методы для защиты информации : учебное пособие / В. Н. Костин. – Москва : МИСиС, 2018. – 40 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=497572. – Текст : электронный.

4. Скрипник, Д. А. Общие вопросы технической защиты информации / Д. А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429070. – Текст : электронный.

5. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 . – Текст : электронный.

8.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*http://www.edu.ru/index.php*
База данных Научной электронной библиотеки eLIBRARY.RU	*https://elibrary.ru/*
Федеральная университетская компьютерная сеть России	*http://www.runnet.ru/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://www.window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*http://minobrnauki.gow.ru*
Портал открытого on-line образования	*http://npoed.ru*
Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов	*http://www.ict.edu.ru/*
Электронная образовательная среда ФГБОУ ВО «ВГУИТ	*http://education.vsuet.ru*
Справочно-правовая система «Консультант+»	*http://www.consultant-urist.ru*
Справочно-правовая система «Гарант»	*http://www.garant.ru*
Базаданных Web of Science	*https://apps.webofknowledge.com/*
База данных Scopus	*https://www.scopus.com*
Портал открытых данных Российской Федерации	*https://data.gov.ru*
База данных профессиональных стандартов Министерства труда и социальной защиты РФ	*http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/*

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Перечень программного обеспечения и информационных справочных систем:

1. Microsoft Office Professional Plus 2010;
2. Microsoft Office Professional Plus 2013;
3. Microsoft Office 2007;
4. Среда разработки MS Visual Studio;
5. СУБД MS SQL Server;
6. Программный пакет «Crypton LITE»;
7. Kerio WinRoute FireWall;
8. сканер безопасности «XSpider»;
9. Страж NT (версия 3.0);
10. Ревизор Сети (10 IP-адресов);
11. Ревизор-2 XP, Ревизор-1 XP;
12. Lazarus;
13. «Российское образование» - федеральный портал https://www.edu.ru/;
14. Научная электронная библиотека https://elibrary.ru/defaultx.asp;
15. Национальная исследовательская компьютерная сеть России https://niks.su/;
16. Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/;
17. Электронная библиотека ВГУИТ http://biblos.vsuet.ru/megapro/web;
18. Сайт Министерства науки и высшего образования РФ https://minobrnauki.gov.ru/;
19. Портал открытого on-line образования https://npoed.ru/;
20. Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ» https://education.vsuet.ru/.

8.3 Методические указания к прохождению практики

8.3.1 Методические указания для обучающихся

Для студентов, обучающихся без использования дистанционных образовательных технологий

Методические рекомендации по организации учебной работы студента направлены на повышение ритмичности и эффективности его самостоятельной работы по практике.

Завершающим этапом практики является подведение ее итогов. Подведение итогов практики **Производственная практика** предусматривает выявление степени выполнения студентом программы практики, полноты и качества собранного материала, наличия необходимого анализа, расчетов, степени обоснованности выводов, выявление недостатков в прохождении практики, представленном материале и его оформлении, разработку мер и путей их устранения.

Студент, получив замечания и рекомендации руководителя практики, после соответствующей доработки, выходит на защиту (зачет) отчета о практике. Отрицательный отзыв о работе студента во время практики, несвоевременная сдача отчета или неудовлетворительная оценка при защите отчета по практике считаются академической задолженностью.

По результатам практики составляется отчет, структура которого определяется задачами, установленными для данного типа практики в соответствии с методическими указаниями по сбору материала.

Цель отчета – показать степень полноты выполнения студентом программы практики. Объем отчета (основной текст) – 25-30 страниц. Таблицы, схемы, рисунки, чертежи можно поместить в приложения, в этом случае в основной объем отчета они не входят.

Структурные элементы отчета по практике **Производственная практика**:

- титульный лист;
- содержание;
- введение;
- основная часть: характеристика предприятий, с деятельностью которых

ознакомился студент во время практики.

− заключение;

− список использованных источников;

− приложения.

При оформлении отчета следует ориентироваться на требования ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления».

Содержание и оформление отчета оценивается в соответствии с принятой в университете рейтинговой системой оценки знаний. Максимальная оценка отчета составляет 60 баллов.

В соответствии с учебным планом прохождение практики завершается итоговым контролем в форме зачета с оценкой. Максимальная оценка на зачете с оценкой составляет 40 баллов.

Общая оценка результатов освоения практики складывается из числа баллов, набранных при оценке отчета по практике и при защите отчета на оценку. Максимальная общая оценка всей практики составляет 100 баллов.

Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий занятия полностью или частично проводятся в режиме онлайн. Объем **практики** и распределение нагрузки по видам работ соответствует разделу 5. Распределение баллов соответствует п. 8.3.1 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего(их) преподавателя(ей)/руководителя(ей) практики и доводится до обучающихся.

8.3.2. Методические рекомендации преподавателям

Основной задачей преподавателей, проводящих практику **Производственная практика,** является инструктаж обучающихся о формах проведения практической подготовки, ознакомление обучающихся с основными задачами профессиональной деятельности.

Перед выездом на практику руководители практики от университета проводят собрания в группах, на которых разъясняют цели, задачи и порядок прохождения практики; знакомят с требованиями к отчетам по практике и порядком сдачи зачета.

Руководитель практики от университета обязан за 1-3 дня до начала практики студентов прибыть на предприятие и решить организационные вопросы. Совместно с руководителем практики от предприятия согласовать календарный план прохождения практики.

По прибытии на предприятие перед началом студенты в обязательном порядке проходят инструктаж по противопожарной безопасности и охране труда, знакомятся с правилами внутреннего распорядка на предприятии.

Работа студентов во время практики должна контролироваться руководителями практики от предприятия и университета в установленном порядке.

Во время посещений предприятий, на базе которых проходит практическая подготовка необходимо обратить внимание студентов на место их будущей профессии на рынке труда и значении на предприятиях различного рода деятельности. Для более глубокого изучения предмета преподаватель предоставляет студентам информацию о возможности использования Интернет-ресурсов по практике.

Для преподавателей, реализующих образовательные программы с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий занятия полностью или частично проводятся в режиме онлайн. Объем **практики** и распределение нагрузки по видам работ соответствует Разделу 5. Распределение баллов соответствует п. 8.3.1 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения

ведущего преподавателя и доводится до обучающихся.

Реализация ЭО и ДОТ предполагает использование следующих видов и учебной деятельности: онлайн консультации, практические занятия, видео-лекции; лабораторные работы, проводимые полностью или частично с применением ЭО и ДОТ; текущий контроль в режиме тестирования и проверки домашних заданий; онлайн консультации; самостоятельная работа и т.д. – в зависимости от рабочей программы практики.

При реализации РПП в зависимости от конкретной ситуации ЭО и ДОТ могут быть применены в следующем виде:

• объем часов контактной работы обучающихся с преподавателем не сокращается и электронные образовательные ресурсы (ЭОР) методически обеспечивают самостоятельную работу обучающихся в объеме, предусмотренном рабочей программой учебной практики. При этом в случае необходимости занятия проводятся в режиме онлайн;

• смешанные формы обучения, сочетающие в себе аудиторные занятия (при возможности перевода части контактных часов работы обучающихся с преподавателем в электронную информационно-образовательную среду без потери содержания учебной практики) и ЭОР (часть учебного материала (например, лекции) может быть заменена ЭОР);

• учебные курсы, интегрированные в LMS Moodle, контактные часы по которым могут быть исключены, изучаются обучающимися самостоятельно при минимальном участии преподавателя (консультации в режиме форума или в режиме вебинара).

9. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на практике

1) Информационно-развивающие технологии:

- использование мультимедийного оборудования при проведении практики;
- получение студентом необходимой учебной информации под руководством преподавателя или самостоятельно;
- метод IT - использование в учебном процессе системы автоматизированного проектирования;

2) Развивающие проблемно-ориентированные технологии.

- проблемные лекции и семинары;
- «работа в команде» - совместная деятельность под руководством лидера, направленная на решение общей поставленной задачи;
- «междисциплинарное обучение» - использование знаний из разных областей, группируемых и концентрируемых в контексте конкретно решаемой задачи;
- контекстное обучение;
- обучение на основе опыта.

3) Личностно ориентированные технологии обучения.

- консультации;
- «индивидуальное обучение» - выстраивание для студента собственной образовательной траектории с учетом интереса и предпочтения студента;
- опережающая самостоятельная работа – изучение студентами нового материала до его изложения преподавателем на лекции и других аудиторных занятиях;
- подготовка к докладам на студенческих конференциях.

10. Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется материально-техническая база кафедры «Информационная безопасность», ее аудиторный фонд, соответствующий санитарным, противопожарным нормам и требованиям техники безопасности. Кафедра располагает наличием компьютерных классов (аудиториями (а. 332а, 420, 424), оснащенными в каждой аудитории 12 ПК Intel Core 2 Duo персональных компьютеров) с выходом в сеть «Интернет» и установленным лицензионным программным обеспечением (Microsoft Windows 8.1, Microsoft Office 2013, AutoCAD, САПР КОМПАС и др.).

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по практике (практической подготовке)

Производственная практика

(Практика по получению профессиональных умений
и опыта профессиональной деятельности)

1 Перечень компетенций с указанием этапов их формирования

№п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК-1	способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	основные понятия и задачи векторной алгебры и аналитической геометрии	определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач	навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач
2	ОПК-2	способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники		применять при решении профессиональных задач с использованием вычислительной техники соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации	расчетными формулами, компьютерными программами при решении математических задач
3	ОПК-3	способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	современные технологии и методы программирования	строить логические и правильные программы	составления программ по разработанным алгоритмам
6	ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах	формы и способы представления данных в персональном компьютере	применять средства восстановления системы после сбоя, чистки и дефрагментации диска	навыками работы с современными информационными технологиями для поиска информации
7	ОПК-5	способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	методы научных исследований в профессиональной деятельности	проводить комплексное проектировать структуру и архитектуру программного обеспечения с использованием современных методологий	
8	ОПК-6	способностью применять нормативные правовые акты в профессиональной деятельности	основы организационного и правового обеспечения информационной безопасности	применять нормативные правовые акты, руководящие и методические документы,	навыками организации и обеспечения режима секретности

				регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла	
9	ОПК-7	способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций	технику безопасности при работе с приборами и оборудованием для защиты информации	работать с офисной техникой и специализированным оборудованием с учетом требований техники безопасности	навыками работы с измерительным и приборами и типовым оборудованием для защиты информации
10	ОПК-8	способностью к освоению новых образцов программных, технических средств и информационных технологий	основные технические и программные средства защиты информации, используемые на предприятии	пользоваться приборами выявления каналов утечки информации, обнаружения подслушивающих устройств и приборов незаконного съема информации, локализации действия средств несанкционированного доступа	методиками проведения аналитической работы по предупреждению утечки конфиденциальной информации
11	ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	предъявляемые в организациях требования к специалистам, работающим в области защиты информации	работать со специализированными прикладными программами, инструментальной системой программирования и ресурсами Интернет	применения руководящих и нормативных документов по инженерно-технической защите информации
12	ПК-2	способностью создавать и исследовать модели автоматизированных систем	основные технологии защиты информации, используемые на предприятии		навыками проектирования программного обеспечения с использованием средств автоматизации
13	ПК-3	способностью проводить анализ защищенности автоматизированных систем	средства обеспечения безопасности данных	применять основные законы и нормативные документы в области информационной безопасности	навыками анализа основных узлов устройств современных автоматизированных систем
14	ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	источники и классификацию угроз информационной безопасности	проводить мониторинг угроз безопасности компьютерных сетей	навыками программирования в профессиональной деятельности
15	ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	основные риски информационной безопасности	планировать политику безопасности операционных систем	навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных

					аппаратных средств автоматизированных систем
16	ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	мировые и российские стандарты в области информационной безопасности	применять на практике методы анализа электрических цепей	навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств
17	ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	принципы организации документирования разработки, процесса сопровождения программного обеспечения	пользоваться нормативными документами но противодействию технической разведке	навыками разработки, документирования, тестирования и отладки программного обеспечения
18	ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем		проводить анализ проектных решений по обеспечению информационной безопасности	профессиональной терминологией в области информационной безопасности
19	ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения	способностью учувствовать в разработке защищенных автоматизированных систем
20	ПК-10	способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	характеристики каналов передачи данных	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей	
21	ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	принципы построения систем защиты информации	участвовать в разработке политики информационной безопасности	планирования политики безопасности операционных систем
22	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	компоненты системы управления информационной безопасностью автоматизированной системы		навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей
23	ПК-13	способностью	методы и средства	проводить выбор	

		участвовать в проектировании средств защиты информации автоматизированной системы	проектирования средств защиты информации	эффективных способов реализации структур данных и конкретных алгоритмов	
24	ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	процесс сопровождения программного обеспечения	участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств	
25	ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	правовые акты по аттестации объектов информатизации и сертификации средств защиты информации	участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации	навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации
26	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	нормативную документацию в области аттестации автоматизированных систем		навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры
27	ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	функции межсетевых экранов, профили защиты для межсетевых экранов		выбора и использования архитектурных особенностей вычислительных систем различных классов
28	ПК-18	способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности		соблюдать правила вежливости и культуры поведения в профессиональной деятельности давать нравственную оценку коррупционным проявлениям и другим нарушениям норм профессиональной этики	навыками конструктивного общения в процессе профессиональной деятельности
29	ПК-19	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		участвовать в разработке предложений по совершенствованию системы управления информационной безопасностью	методами формирования требований по защите информации
30	ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем		навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности

		безопасности			
31	ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	участвовать в коллективной разработке проектов документов по обеспечению информационной безопасности	
32	ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	задачи систем анализа защищенности в защите открытых систем	применять принципы формирования политики информационной безопасности	
33	ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	состав информации ограниченного доступа организации	применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационны х систем	
34	ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	слабости системных утилит, команд и сетевых сервисов	применять математические методы при решении профессиональных задач моделирования повышенной сложности	
35	ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций		использовать частные и обобщенные модели систем комплексной защиты информации	навыками работы с сетевыми сканерами, сканерами безопасности
36	ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	методы, принципы, процедуры и службы администрирования информационных систем	участвовать в администрировании подсистемы информационной безопасности	средствами SQL Server для администрирова ния удаленных баз данных
37	ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности	основные протоколы компьютерных сетей	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных	

		автоматизированной системы			
38	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования	участвовать в работе коллектива по управлению информационной безопасностью организации	
39	ПСК-4.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	комплексном подходе к построению эшелонированной защиты для автоматизированных систем		навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия
40	ПСК-4.2	способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	понятия информационной безопасности, защиты информации, назначение и основные возможности систем защиты информации	открывать и закрывать общий доступ к информации в локальной сети	
41	ПСК-4.3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	основные компоненты архитектуры мобильных платформ	устранять источники угроз безопасности мобильных систем и приложений	навыками программирования простейших методов шифрования-дешифрования
42	ПСК-4.4	способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	терминологию и системный подход построения защищенных открытых информационных систем	проектировать взаимодействия многомашинных информационных систем, используя стандартные протоколы эталонной модели	навыками оценивания стойкости различных паролей
43	ПСК-4.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	принципы декодирования HTTP	создавать CGI, ISAPI и WEB приложения	навыками формирования ключей шифрования с заданной стойкостью

2 Паспорт оценочных материалов по дисциплине

№ п/п	Показатель	Способ (технология) оценивания	Описание шкалы оценивания
1	Отчет по практике	Проверка преподавателем	Отлично, хорошо, удовлетворительно, неудовлетворительно
2	Собеседование (защита отчета по практике)	Проверка преподавателем	Отлично, хорошо, удовлетворительно,

			неудовлетворительно

3. Оценочные материалы для промежуточной аттестации

3.1. Отчет по практике

№	Формулировка задания (разделы отчета)
1	аналитический обзор нормативно-правовой документации предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения, на котором проводится практика
2	описание видов, методов, средств информационной защиты, применяемых на предприятии
3	выполнение установки, настройки или эксплуатации компонентов системы обеспечения информационной безопасности согласно индивидуальным задачам производственной практики

3.2. Собеседование (защита отчета по практике)

№	Примерные вопросы
1	Основные типы несанкционированного доступа к компонентам автоматизированных систем.
2	Модели разграничения доступа. Сущность и основные свойства модели матрицы доступов.
3	Идентификация и аутентификация субъектов доступа с помощью имени и пароля.
4	Аутентификация с использованием внешних носителей информации
5	Методы подбора паролей
6	Основные компоненты информационной системы подверженные атакам
7	Основные методы и средства защиты от удаленных атак
8	Назначение и функции подсистемы аудита
9	Методы поиска функций защиты в машинном коде.
10	Методы противодействия исследованию алгоритма работы системы защиты.

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 – 2015 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 2012 Положение о рейтинговой оценке текущей успеваемости.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ЗНАТЬ: - основные понятия и задачи векторной алгебры и аналитической геометрии (ОПК-1); - современные технологии и методы программирования (ОПК-3); - формы и способы представления данных в персональном компьютере (ОПК-4); - методы научных исследований в профессиональной деятельности (ОПК-5); - основы организационного и правового обеспечения информационной безопасности (ОПК-6); - технику безопасности при работе с приборами и оборудованием для защиты информации (ОПК-7); - основные технические и программные средства защиты информации, используемые на предприятии (ОПК-8); - предъявляемые в организациях требования к специалистам, работающим в области защиты информации (ПК-1); - основные технологии защиты информации, используемые на предприятии (ПК-2); - средства обеспечения безопасности данных (ПК-3); - источники и классификацию угроз информационной безопасности (ПК-4); - основные риски информационной безопасности (ПК-5); - мировые и российские стандарты в области информационной безопасности (ПК-6); - принципы организации документирования	Собеседование при защите отчета	Уровень владения материалом	При собеседовании обучающийся показывает знание материалов отчета. Полно раскрывает сущность вопроса. Дает исчерпывающие ответы на поставленные вопросы	Отлично 85-100%	Освоена (повышенный)
			При собеседовании обучающийся показывает знание материалов отчета. Достаточно раскрывает сущность вопроса. Отвечает на поставленные вопросы	Хорошо 75-84,99%	Освоена (повышенный)
			При собеседовании обучающийся показывает знание материалов отчета. Недостаточно раскрывает сущность вопроса. Отвечает на поставленные вопросы с ошибками	Удовлетворительно 60-74,99%	Освоена (базовый)
			При собеседовании обучающийся показывает незнание материалов отчета. Не раскрывает сущность вопроса. Не отвечает на поставленные вопросы.	Неудовлетворительно 0-59,99%	Не освоена (недостаточный)

разработки, процесса сопровождения программного обеспечения (ПК-7); - характеристики каналов передачи данных (ПК-10); - принципы построения систем защиты информации (ПК-11); - компоненты системы управления информационной безопасностью автоматизированной системы (ПК-12); - методы и средства проектирования средств защиты информации (ПК-13); - процесс сопровождения программного обеспечения (ПК-14); - правовые акты по аттестации объектов информатизации и сертификации средств защиты информации (ПК-15); - нормативную документацию в области аттестации автоматизированных систем (ПК-16); - функции межсетевых экранов, профили защиты для межсетевых экранов (ПК-17); - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем (ПК-20); - разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21); - задачи систем анализа защищенности в защите открытых систем (ПК-22); - состав информации ограниченного доступа организации (ПК-23); - слабости системных утилит, команд и сетевых сервисов (ПК-24); - методы, принципы, процедуры и службы администрирования информационных систем (ПК-26); - основные протоколы компьютерных сетей					

(ПК-27); - технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования (ПК-28); - комплексном подходе к построению эшелонированной защиты для автоматизированных систем (ПСК-4.1); - понятия информационной безопасности, защиты информации, назначение и основные возможности систем защиты информации (ПСК-4.2); - основные компоненты архитектуры мобильных платформ (ПСК-4.3); - терминологию и системный подход построения защищенных открытых информационных систем (ПСК-4.4); - принципы декодирования HTTP (ПСК-4.5)					
УМЕТЬ: - определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач (ОПК-1); - применять при решении профессиональных задач с использованием вычислительной техники соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации (ОПК-2); - строить логические и правильные программы (ОПК-3); - применять средства восстановления системы после сбоя, чистки и дефрагментации диска (ОПК-4); - проводить комплексное проектировать структуру и архитектуру программного обеспечения с использованием современных методологий (ОПК-5);	Выполнение отчета	Применение полученных знаний при выполнении отчета	Отчет выполнен и оформлен по установленным требованиям без замечаний, полностью раскрыты все пункты отчета. Показан высокий уровень владения информацией. Отчет сдан в срок	Отлично 85-100%	Освоена (повышенный)
			Отчет выполнен и оформлен по установленным требованиям, но имеются незначительные замечания по тексту и оформлению отчета. Показан достаточный уровень владения информацией. Отчет сдан в срок	Хорошо 75-84,99%	Освоена (повышенный)
			Отчет в целом выполнен, но имеются замечания по тексту и оформлению работы. Показан невысокий уровень владения информацией. Отчет сдан в срок.	Удовлетворительно 60-74,99%	Освоена (базовый)
			Отчет не выполнен по установленным требованиям, имеются значительные замечания по тексту и оформлению работы. Обучающийся не владеет информацией	Неудовлетворительно 0-59,99%	Не освоена (недостаточный)

- применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ОПК-6); - работать с офисной техникой и специализированным оборудованием с учетом требований техники безопасности (ОПК-7); - пользоваться приборами выявления каналов утечки информации, обнаружения подслушивающих устройств и приборов незаконного съема информации, локализации действия средств несанкционированного доступа (ОПК-8); - работать со специализированными прикладными программами, инструментальной системой программирования и ресурсами Интернет (ПК-1); - применять основные законы и нормативные документы в области информационной безопасности (ПК-3); - проводить мониторинг угроз безопасности компьютерных сетей (ПК-4); - планировать политику безопасности операционных систем (ПК-5); - применять на практике методы анализа электрических цепей (ПК-6); - пользоваться нормативными документами но противодействию технической разведке (ПК-7); - проводить анализ проектных решений по обеспечению информационной безопасности (ПК-8); - формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения (ПК-9);					

- анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей (ПК-10); - участвовать в разработке политики информационной безопасности (ПК-11); - проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов (ПК-13); - участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств (ПК-14); - участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15); - соблюдать правила вежливости и культуры поведения в профессиональной деятельности давать нравственную оценку коррупционным проявлениям и другим нарушениям норм профессиональной этики (ПК-18); - участвовать в разработке предложений по совершенствованию системы управления информационной безопасностью (ПК-19); - участвовать в коллективной разработке проектов документов по обеспечению информационной безопасности (ПК-21); - применять принципы формирования политики информационной безопасности (ПК-22); - применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем (ПК-23); - применять математические методы при решении профессиональных задач моделирования повышенной сложности (ПК-24);					

- использовать частные и обобщенные модели систем комплексной защиты информации (ПК-25); - участвовать в администрировании подсистемы информационной безопасности (ПК-26); - разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных (ПК-27); - участвовать в работе коллектива по управлению информационной безопасностью организации (ПК-28); - открывать и закрывать общий доступ к информации в локальной сети (ПСК-4.2); - устранять источники угроз безопасности мобильных систем и приложений (ПСК-4.3); - проектировать взаимодействия многомашинных информационных систем, используя стандартные протоколы эталонной модели (ПСК-4.4); - создавать CGI, ISAPI и WEB приложения (ПСК-4.5)					
ВЛАДЕТЬ: - навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач (ОПК-1); - расчетными формулами, компьютерными программами при решении математических задач (ОПК-2); - составления программ по разработанным алгоритмам (ОПК-3); - навыками работы с современными информационными технологиями для поиска информации (ОПК-4); - навыками организации и обеспечения режима секретности (ОПК-6); - навыками работы с измерительными приборами и типовым оборудованием для защиты информации (ОПК-7);	Защита отчета	Демонстрация полученных знаний в процессе защиты отчета (презентации)	Обучающийся демонстрирует системность и глубину полученных знаний. Грамотно и логически излагает материал по теме отчета. Правильно отвечает на все вопросы преподавателя	Отлично 85-100%	Освоена (повышенный)
			Обучающийся демонстрирует достаточную точность и полноту знаний в объеме программы практики. Владеет необходимой терминологией и логически излагает материал по теме отчета. Отвечает на вопросы преподавателя, допуская неточности	Хорошо 75-84,99%	Освоена (повышенный)
			Обучающийся демонстрирует недостаточную полноту знаний в объеме программы практики. Плохо владеет необходимой терминологией. Материал излагает нелогично.	Удовлетворительно 60-74,99%	Освоена (базовый)

- методиками проведения аналитической работы по предупреждению утечки конфиденциальной информации (ОПК-8); - применения руководящих и нормативных документов по инженерно-технической защите информации (ПК-1); - навыками проектирования программного обеспечения с использованием средств автоматизации (ПК-2); - навыками анализа основных узлов устройств современных автоматизированных систем (ПК-3); - навыками программирования в профессиональной деятельности (ПК-4); - навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем (ПК-5); - навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств (ПК-6); - навыками разработки, документирования, тестирования и отладки программного обеспечения (ПК-7); - профессиональной терминологией в области информационной безопасности (ПК-8); - способностью учувствовать в разработке защищенных автоматизированных систем (ПК-9); - планирования политики безопасности операционных систем (ПК-11); - навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей (ПК-12); - навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15); - навыками использования измерительного			Отвечает на вопросы преподавателя с ошибками		
			Обучающийся демонстрирует фрагментарные знания по программе практики. Не владеет необходимой терминологией. Материал излагает нелогично. Не отвечает на вопросы преподавателя.	Неудовлетворительно 0-59,99%	Не освоена (недостаточный)

оборудования при экспериментальном исследовании электронной аппаратуры (ПК-16); - выбора и использования архитектурных особенностей вычислительных систем различных классов (ПК-17); - навыками конструктивного общения в процессе профессиональной деятельности (ПК-18); - методами формирования требований по защите информации (ПК-19); - навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности (ПК-20); - навыками работы с сетевыми сканерами, сканерами безопасности (ПК-25); - средствами SQL Server для администрирования удаленных баз данных (ПК-26); - навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия (ПСК-4.1); - навыками программирования простейших методов шифрования-дешифрования (ПСК-4.3); - навыками оценивания стойкости различных паролей (ПСК-4.4); - навыками формирования ключей шифрования с заданной стойкостью (ПСК-4.5)					