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.
(подпись) (Ф.И.О.)

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ ПРАКТИКА)

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели 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.

2. Задачи практики

– сбор, обработка и анализ материала для выполнения выпускной квалификационной работы;

– реализация опыта создания и применения информационных технологий и систем информационного обеспечения;

– совершенствование навыков решения информационных задач на конкретном рабочем месте.

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.

3. Место практики в структуре образовательной программы

3.1. Преддипломная практика 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.

3.2. Для успешного прохождения практики необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Производственная практика», «Администрирование в информационных системах», «Аудит информационных технологий и систем обеспечения информационной безопасности».

Для освоения производственной практики студент должен:

– знать методы защиты информации;

– уметь пользоваться приемами локализации действия средств несанкционированного доступа;

– владеть средствами информационной безопасности.

3.3. Знания, умения и навыки, сформированные при прохождении практики, необходимы для успешной защиты ВКР.

4. 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 использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

– способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

– способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

– способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

– 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).

В результате прохождения практики обучающийся должен:

Знать:

– основные тенденции развития экономической системы общества (ОК-2);

– конституционные права и обязанности человека и гражданина РФ (ОК-4);

– основы обеспечения информационной безопасности (ОК-5);

– 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);

– нормативно-правовую базу организации работы персонала по защите информации (ПСК-4.1);

– методологию разработки политики информационной безопасности (ПСК-4.2);

– основные методы научных исследований в области управления информационной безопасностью (ПСК-4.3);

Уметь:

– применять философские знания для формирования мировоззренческой позиции (ОК-1);

– анализировать информацию, характеризующую основные тенденции развития экономической системы общества (ОК-2);

– анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности (ОК-3);

– применять нормы конституционного права руководствуясь принципами законности и патриотизма (ОК-4);

– 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);

– Применять нормативную документацию предприятия по обеспечению информационной безопасности (ПСК-4.1);

– Реализовывать политику информационной безопасности (ПСК-4.2);

– Оценивать различные инструменты в области проектирования и управления информационной безопасностью (ПСК-4.3);

Владеть:

– навыками философского анализа различных профессиональных проблем (ОК-1);

– навыками письменного аргументированного изложения собственной точки зрения (ОК-3);

– мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности (ОК-5);

– 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 защиты персональных данных сотрудников предприятия (ПСК-4.1);

– Применения технологии автоматизации информационных процессов (ПСК-4.2);

– Применения различных информационных систем при проектировании, эксплуатации и совершенствовании систем управления информационной безопасностью (ПСК-4.3).

5. Способы и форма(ы) проведения практики

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.

6. Структура и содержание практики

6.1. Содержание разделов практики

1) аналитический обзор бизнес-процессов предприятия, нормативной документации предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения, на котором проводится практика;

2) описание задач, эффективность решения которых можно повысить за счет внедрения автоматизированных информационных систем, либо проблем, возникающих при использовании информационных технологий на базе практики.

6.2 Распределение часов по семестрам и видам работ по практике

Общая трудоемкость прохождения практики составляет 13 з.е., 468 академических часов, 8 2/3 недели. Контактная работа обучающегося (КРо) составляет 312 ч. Иные формы работы 156 ч.

7. 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.

8. Оценочные материалы для промежуточной аттестации обучающихся по практике

8.1. 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.

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

9. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения 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. Халабия, Р. Ф. Организация ЭВМ и вычислительных систем : методические указания / Р. Ф. Халабия, И. В. Степанова, Е. И. Зайцев. – Москва : РТУ МИРЭА, 2021. – 96 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/226637. – Режим доступа: для авториз. пользователей.

2. Артюшенко, В. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / В. В. Артюшенко, А. В. Никулин. – Новосибирск : НГТУ, 2020. – 72 с. – ISBN 978-5-7782-4104-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/152244 – Режим доступа: для авториз. пользователей.

3. Гриценко, Ю. Б. Вычислительные системы, сети и телекоммуникации : учебное пособие / Ю. Б. Гриценко. – Москва : ТУСУР, 2015. – 134 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/110295 – Режим доступа: для авториз. пользователей.

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.

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

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.

11. 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/.

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

Для проведения практики используется материально-техническая база кафедры информационной безопасности, 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.).

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по практике (практической подготовке)

Производственная практика (преддипломная практика)

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	ОК-1	способностью использовать основы философских знаний для формирования мировоззренческой позиции		применять философские знания для формирования мировоззренческой позиции	навыками философского анализа различных профессиональных проблем
2	ОК-2	способностью использовать основы экономических знаний в различных сферах деятельности	основные тенденции развития экономической системы общества	анализировать информацию, характеризующую основные тенденции развития экономической системы общества	
3	ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма		анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности	навыками письменного аргументированного изложения собственной точки зрения
6	ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	конституционные права и обязанности человека и гражданина РФ	применять нормы конституционного права руководствуясь принципами законности и патриотизма	
7	ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	основы обеспечения информационной безопасности		мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
8	ОПК-1	способностью анализировать физические явления и процессы, применять соответствующий	основные понятия и задачи векторной алгебры и аналитической геометрии	определять возможности применения теоретических положений и методов	навыками использования стандартных методов и моделей математическо

		математический аппарат для формализации и решения профессиональных задач		математических дисциплин для постановки и решения конкретных прикладных задач	го анализа и их применения к решению прикладных задач
9	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
10	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
11	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
12	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	

13	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, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла	навыками организации и обеспечения режима секретности
14	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 измерительными приборами и типовым оборудованием для защиты информации
15	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
16	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
17	ПК-2	способностью создавать и исследовать модели автоматизированных систем	основные технологии защиты информации, используемые на предприятии		навыками проектирования программного обеспечения с использованием средств автоматизации

18	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
19	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
20	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
21	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
22	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
23	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
24	ПК-9	способностью участвовать в разработке		формировать требования и разрабатывать	способностью учувствовать в разработке

		защищенных автоматизированных систем в сфере профессиональной деятельности		внешние спецификации для разрабатываемого программного обеспечения	защищенных автоматизированных систем
25	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	
26	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
27	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
28	ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	методы и средства проектирования средств защиты информации	проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов	
29	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	
30	ПК-15	способностью участвовать в проведении экспериментально-исследовательских	правовые акты по аттестации объектов информатизации и сертификации	участвовать в проведении экспериментально-исследовательских работ при	навыками проведения экспериментально-исследователь

		работ при сертификации средств защиты информации автоматизированных систем	средств защиты информации	сертификации средств защиты информации	ских работ при сертификации средств защиты информации
31	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
32	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
33	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
34	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
35	ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем		навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности
36	ПК-21	способностью разрабатывать	разрабатывать проекты	участвовать в коллективной	

		проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	разработке проектов документов по обеспечению информационной безопасности	
37	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	
38	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 телекоммуникационных систем	
39	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	
40	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
41	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 администрирования удаленных баз данных
42	ПК-27	способностью	основные	разрабатывать и	

		выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	протоколы компьютерных сетей	администрировать базы данных и интерфейсы прикладных программ к базам данных	
43	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	
44	ПСК-4.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	нормативно-правовую базу организации работы персонала по защите информации	Применять нормативную документацию предприятия по обеспечению информационной безопасности	Навыками защиты персональных данных сотрудников предприятия
45	ПСК-4.2	способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Методологию разработки политики информационной безопасности	Реализовывать политику информационной безопасности	Применения технологии автоматизации информационных процессов
46	ПСК-4.3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	Основные методы научных исследований в области управления информационной безопасностью	Оценивать различные инструменты в области проектирования и управления информационной безопасностью	Применения различных информационных систем при проектировании, эксплуатации и совершенствовании систем управления информационной безопасностью

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 материалов для промежуточной аттестации

3.1. Отчет по практике

№	Формулировка задания (разделы отчета)
1	аналитический обзор бизнес-процессов предприятия, нормативной документации предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения, на котором проводится практика
2	описание задач, эффективность решения которых можно повысить за счет внедрения автоматизированных информационных систем, либо проблем, возникающих при использовании информационных технологий на базе практики

3.2. Собеседование (защита отчета по практике)

№	Примерные вопросы
1	Должностные права и обязанности, выполняемые функции
2	Основные положения концепции безопасности предприятия
3	Архитектура и топология компьютерной сети предприятия
4	Используемое системное программное обеспечение
5	Используемое прикладное программное обеспечение
6	Предложения по автоматизации процессов обработки информации
7	Предложения по повышению уровня безопасности
8	Программные и аппаратные особенности различных способов организации сетей
9	Проблемы синхронизации, кодирования данных в канале
10	Основные уязвимости открытых информационных систем
11	Методы решения задач анализа систем и процессов защиты информации.
12	Классификация и характеристика методов решения задач анализа систем и процессов защиты информации.
13	Основные состояния системы защиты информации.
14	Этапы решения оптимизационных задач в сфере защиты информации.
15	Системная классификация методов поиска оптимизационных решений.
16	Структурированные компоненты систем защиты информации.
17	Принципы структуризации при разработке систем защиты информации.
18	Определения понятий «модель», «моделирование» и «обобщенная модель».
19	Этапы процесса моделирования системы защиты информации.
20	Общие свойства моделей защиты информации.

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 – Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 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 тенденции развития экономической системы общества (ОК-2); - конституционные права и обязанности человека и гражданина РФ (ОК-4); - основы обеспечения информационной безопасности (ОК-5); - 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	Собеседование при защите отчета	Уровень владения материалом	Отчет оформлен в соответствии с требованиями, замечаний нет, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			Отчет оформлен в соответствии с требованиями, имеются некоторые замечания, ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (продвинутый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, допустил более 5 ошибок	Не удовлетворительно	Не освоена (недостаточный)

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); - нормативно-правовую базу организации работы персонала по защите информации (ПСК-4.1); - методологию разработки политики информационной безопасности (ПСК-4.2); - основные методы научных исследований в области управления информационной безопасностью (ПСК-4.3)					
УМЕТЬ: - применять философские знания для формирования мировоззренческой позиции (ОК-1); - анализировать информацию, характеризующую основные тенденции развития экономической системы общества (ОК-2); - анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности (ОК-3); - применять нормы конституционного права руководствуясь принципами законности и патриотизма (ОК-4); - определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач (ОПК-1); - применять при решении профессиональных задач с	Отчет по практике	Подготовка и оформление отчета	Отчет оформлен в соответствии с требованиями, замечаний нет, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			Отчет оформлен в соответствии с требованиями, имеются некоторые замечания, ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (продвинутый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)

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); - Применять нормативную документацию предприятия по обеспечению информационной безопасности (ПСК-4.1);					

- Реализовывать политику информационной безопасности (ПСК-4.2); - Оценивать различные инструменты в области проектирования и управления информационной безопасностью (ПСК-4.3)					
ВЛАДЕТЬ: - навыками философского анализа различных профессиональных проблем (ОК-1); - навыками письменного аргументированного изложения собственной точки зрения (ОК-3); - мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности (ОК-5); - 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);	Отчет по практике	Подготовка и оформление отчета	Отчет оформлен в соответствии с требованиями, замечаний нет, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			Отчет оформлен в соответствии с требованиями, имеются некоторые замечания, ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (продвинутый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			Отчет не оформлен в соответствии с требованиями, имеются замечания, ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)

- 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 защиты персональных данных сотрудников предприятия (ПСК-4.1); - Применения технологии автоматизации информационных процессов (ПСК-4.2); - Применения различных информационных систем при проектировании, эксплуатации и совершенствовании систем управления информационной безопасностью (ПСК-4.3)					