Минобрнауки России
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
(ФГБОУ ВО «СГУ им. Питирима Сорокина»)

УТВЕРЖДАЮ
И.о. ректора
_____ Н.А. Михальченкова
«1» июня 2016 г.

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ: ПРАКТИКА ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И НАВЫКОВ

Направление подготовки
10.03.01 (090900) Информационная безопасность

Квалификация (степень) выпускника
Бакалавр

Сыктывкар 2016

1. Вид практики: (тип), способы и формы проведения практики.

Вид практики: учебная.

Способы проведения учебной практики: стационарная.

Тип практики: практика по получению первичных профессиональных умений и навыков.

Учебная практика по получению первичных профессиональных умений и навыков проводится рассредоточено: продолжительностью 1 день в неделю, в течение 12 недель в 5 семестре.

2. Цель учебной практики по получению первичных профессиональных умений и навыков и планируемые результаты практики.

Целью учебной практики по получению первичных профессиональных умений и навыков является:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла базовой и вариативной частей, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;
- изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

Задачи учебной практики по получению первичных профессиональных умений и навыков:

- закрепление на практике знаний, умений и навыков, полученных в процессе теоретического обучения;
- развитие профессиональных навыков и навыков деловой коммуникации;
- сбор необходимых материалов для написания отчета по практике.

Данные задачи учебной практики, соотносятся со следующими **видами** и **задачами** профессиональной деятельности:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

организационно-управленческая деятельность:

организация работы малых коллективов исполнителей с учетом требований защиты информации.

ПАСПОРТ КОМПЕТЕНЦИЙ

Код компетенции	*КОД контролируемой компетенции/или ее части/ формулировка компетенции*	*Перечень планируемых результатов*
ОК	способностью к кооперации с коллегами, работе в коллективе (ОК-5);	*Знать: должностные обязанности сотрудников в области защиты информации.* *Уметь:* *работать в команде, распределять обязанности по выполнению работ.*
ОК	- способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);	*Знать: основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ;* *основные понятия и методы в области управленческой деятельности.* *Уметь: опознавать нестандартные ситуации, использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации, нести персональную ответственность за нарушения нормативно-правовых требований, предпринимать необходимые меры по восстановлению нарушенных прав.*
ОК	- способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-7);	*Знать: место своей будущей профессии в обществе.* *Уметь: находить управленческие решения в профессиональной деятельности.*
ОК	- способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);	*Знать: методы выбора направления и проведения научного исследования;* *порядок оформления и представления результатов научной работы;* *Уметь: определять цель и задачи предметной области, делать обоснованные выводы.*
ОК	- способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);	*Знать: грамматические нормы русского языка и стилистических оборотов речи.* *Уметь: делать четкие, обоснованные выводы, быстро передавать и воспринимать определенное содержание информации.*
ОК	- способностью к саморазвитию, самореализации, приобретению новых	*Знать: формы и методы профессионального развития своей*

	знаний, повышению своей квалификации и мастерства (ОК-11);	*индивидуальности.* *Уметь: усваивать определенные совокупности знаний, умений, навыков и приобретать профессионально-значимые качества.*
ОК	- способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);	*Знать: систему критериев коллективной оценки публичных выступлений.* *Уметь: демонстрировать способность участвовать в дискуссиях и отстаивать свою точку зрения оперируя базой знаний.*
ПК	- способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);	*Знать*: *основные естественнонаучные законы.* *Уметь: использовать знания об основных естественнонаучных закономерностях в решении задач анализа и разработки систем информационной безопасности, применять математические методы в процессах диагностики состояния сложных организационно-технологических систем, правильно производить вычисления.*
ПК	- способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);	*Знать: виды источников информации, средства информационных технологий.* *Уметь: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.*
ПК	- способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);	*Знать: требования нормативных правовых документов в своей профессиональной области.* *Уметь: использовать в практической деятельности правовые знания; анализировать основные правовые акты и осуществлять правовую оценку информации*
ПК	- способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);	*Знать: меры по обеспечению информационной безопасности; принципы организации информационных систем в соответствии с требованиями по защите информации;* *Уметь:* ф*ормулировать политику безопасности, осуществлять меры противодействия нарушениям, анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации;*

		анализировать и оценивать степень риска проявления факторов опасности системы
ПК	- способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);	*Знать: организационную структуру объекта защиты, факторы, воздействующие на объект защиты информации, структуру систем документационного обеспечения;* *Уметь:* ф*ормулировать политику безопасности, осуществлять меры противодействия нарушениям, анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; анализировать и оценивать степень риска проявления факторов опасности системы*
ПК	- способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-8);	*Знать: виды информации и ее носителей, классификацию угроз информации, уязвимости информации, структуру и содержание информационных процессов предприятия, технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.* *Уметь: анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать нормативно-методические документы по защите информации.*
ПК	- способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);	*Знать: функции подсистем управления информационной безопасностью на предприятии.* *Уметь: использовать различные программные и аппаратные средства защиты; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;*
ПК	способностью администрировать подсистемы информационной безопасности объекта (ПК-10);	*Знать: аппаратные средства вычислительной техники, операционные системы, основы администрирования автоматизированных систем.* *Уметь: проводить анализ сетевого трафика, применять программно-аппаратные средства защиты информации.*
ПК	- способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных	*Знать: аппаратные средства вычислительной техники; операционные системы, основы*

	средств защиты информации (ПК-11);	*администрирования вычислительных сетей; системы управления базами данных.* *Уметь: настраивать и обслуживать средства защиты информации.*
ПК	- способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);	*Знать: современные средства разработки и анализа программного обеспечения, принципы построения информационных систем;* *Уметь: применять программные средства обеспечения защиты информации.*
ПК	- способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);	*Знать: методы оценки угроз и степени риска.* *Уметь: проводить технико-экономический анализ решений по обеспечению информационной безопасности.*
ПК	- способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);	*Знать: структуру систем документационного обеспечения;* *Уметь: оформлять техническую и методическую документацию в области информационной безопасности.*
ПК	- способностью применять программные средства системного, прикладного и специального назначения (ПК-15);	*Знать: современные средства разработки и анализа программного обеспечения, операционные системы, правовые нормы по вопросам сертификации и лицензирования в области защиты информации.* *Уметь: применять программные средства системного, прикладного и специального назначения.*
ПК	- способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);	*Знать: методы программирования и методы разработки эффективных алгоритмов решения прикладных задач.* *Уметь: использовать инструментальные средства и системы программирования.* *Владеть: методикой программирования для решения профессиональных задач.*
ПК	- способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);	*Знать: методики проведения аудита в области информационной безопасности.* *Уметь: применять методики проведения аудита в области информационной безопасности.*
ПК	- способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);	*Знать: методы получения и сбора значимой информации.* *Уметь: делать выводы на основании проведенного анализа.*
ПК	- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения	*Знать: виды источников и носителей информации.* *Уметь: обобщать большие объемы информации, полученные в результате*

	информационной безопасности (ПК-24);	*изучения различных источников.*
ПК	- способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);	*Знать: сравнительные характеристики профессиональной деятельности организаций различных форм собственности.* *Уметь: обобщать опыт работы других организаций, изученный по открытым источникам информации.*
ПК	- способностью участвовать в работах по реализации политики информационной безопасности (ПК-29);	*Знать: возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, специфику деятельности объекта защиты, методы документирования информации.* *Уметь: определять функции взаимодействия структурных подразделений, разрабатывать политику информационной безопасности объекта защиты.*
ПК	- способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);	*Знать: требования по охране труда и технике безопасности.* *Уметь: анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.*

3. Место учебной практики по получению первичных профессиональных умений и навыков в структуре ООП ВО

Учебной практика по получению первичных профессиональных умений и навыков относится к *вариативной* части программы бакалавриата по направлению подготовки «090900 Информационная безопасность» и профилю подготовки «Комплексная защита объектов информатизации».

В соответствии с ФГОС ВО по направлению подготовки 090900 «Информационная безопасность» раздел основной образовательной программы бакалавриата «Учебная и производственная практики» является обязательным. Учебная практика представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся, закрепляет знания и умения, приобретаемые обучающимися в результате освоения теоретических курсов, вырабатывает практические навыки и способствуют комплексному формированию общекультурных и профессиональных компетенций обучающихся.

Учебной практике предшествуют курсы «Математики», «Информатики», «Экономики», «Иностранный язык», «Структуры и основы деятельности предприятий различных форм собственности», «Физики», «Концепции современного естествознания», «Математическая логика и теория алгоритмов», «Безопасность жизнедеятельности», «Документоведение», «Основы программирования», «Основы информационных технологий», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Языки программирования», «Электротехника», «Операционные системы и оболочки», «Операционная система Linux», «История российских спецслужб», «Математические основы криптологии», «Информационные технологии», «Информационная безопасность автоматизированных систем», «Инженерно-техническая защита информации», «Электрорадиоизмерения», «Основы

радиотехники», «Экономика защиты информации», «Управление рисками», «Базы данных», «Web-программирование» предполагающих проведение лекционных и семинарских занятий с обязательным итоговым контролем в форме зачетов и экзаменов.

Требования к входным знаниям, умениям и готовности студентов, приобретенных в результате освоения предшествующих частей ООП: студент должен

знать:

основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений, основные понятия и методы математического анализа, основные понятия, законы и модели электричества и магнетизма, особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности, основные понятия информатики, место и роль информационной безопасности в системе национальной безопасности РФ, методы программирования, аппаратные средства вычислительной техники, операционные системы персональных ЭВМ, принципы построения информационных систем, системы управления базами данных, структуру систем документационного обеспечения, технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы протекающие в них,

быть готовым к:

оценке эффективности управленческих решений, письменному изложению собственной точки зрения, ведению дискуссий и полемике, владению иностранным языком, в объеме, необходимом для получения информации по профессиональной тематике, использованию программных и аппаратных средств персонального компьютера, поиску информации в глобальной информационной сети Интернет и работы с офисными приложениями, выбору необходимых инструментальных средств для разработки программ в различных операционных системах, составлению, тестированию и отлаживанию программ на языках высокого уровня, оценке угроз информационной безопасности объекта, использованию профессиональной терминологии, выявлению и уничтожению компьютерных вирусов, формулировать и настраивать Политику безопасности распространенных операционных систем, осуществлению мер противодействия нарушениям информационной безопасности с использованием аппаратных и программных средств защиты, применять отечественные и зарубежные стандарты в области безопасности, выявлению угроз безопасности АС, использованию методов технической защиты информации, проведению расчетов и инструментального контроля показателей технической защиты информации.

4. Объём учебной практики по получению первичных профессиональных умений и навыков и ее продолжительность

Общая трудоемкость учебной практики составляет 3 зачетных единицы, 108 часов. Учебная практика проходит в 5 семестре, 1 день в неделю, в течение 12 недель.

Учебная практика проходит в СГУ им. Питирима Сорокина на базе кафедры информационной безопасности в лаборатории ИТЗИ, в лаборатории ПАЗИ, на базе Регионального аттестационного центра, на базе Управления по безопасности и на базе Управления информатизации СГУ им. Питирима Сорокина.

Руководство практикой осуществляют преподаватели кафедры информационной безопасности.

5. Содержание учебной практики по получению первичных профессиональных умений и навыков

№	Этапы практики	Содержание деятельности	Формы текущего контроля

п/п			(отчетности)
1	Ознакомительно-подготовительный	- Общее собрание обучающихся по вопросам организации учебной практики; - инструктаж по технике безопасности; - ознакомление их с программой учебной практики, целями и задачами практики; - ознакомление с организацией прохождения практики; - ознакомление с тематикой индивидуальных заданий; - ознакомление обучающегося с формой и видом отчетности; - ознакомление с порядком защиты отчета по учебной практике и требованиями к оформлению отчета по учебной практике; - подбор материала для прохождения практики.	Распоряжение о допуске к прохождению практики. Присутствие на установочной конференции.
2	Деятельностный	Выполнение практических заданий. Работа с измерительными приборами. Сбор материалов для отчетной документации.	Требования. Рекомендации. Пошаговый анализ выполнения практических заданий. Оформление отчетной документации – ежедневно. Проверка промежуточных отчетов по выполнению практических заданий.
3	Оценочно-результативный	Систематизация и анализ выполненных заданий. Оформление отчетной документации.	Анализ отчетной документации за период практики. Отчет о прохождении практики на итоговой конференции. Оценка работы.

Учебная практика студентов проводится в форме самостоятельной практической работы под руководством преподавателя.

Студент при прохождении практики получает от руководителя указания, рекомендации и разъяснения по всем вопросам, связанным с организацией и прохождением практики, отчитывается о выполняемой работе в соответствии с практическим заданием практики.

6. Формы отчетности по учебной практике по получению первичных профессиональных умений и навыков

Формы отчетности по практике	*Отчеты по выполнению практических заданий; Итоговый отчет о прохождении учебной практики.*
*Сроки получения допуска к прохождению практики (*Инструктаж по технике безопасности и пожарной безопасности обучающиеся получают от руководителя практики и расписываются в журнале*);*	*За месяц до начала практики*
Сроки проведения установочной конференции	*За месяц до начала практики*

по практике;	
Сроки сдачи документов по практике для проверки в институт;	*В течение недели после окончания практики*
Сроки проведения итоговой конференции по практике.	*В течение месяца после окончания практики. Сроки итоговой конференции устанавливаются распоряжением директора института.*
Форма итогового контроля по практике.	*Защита итогового отчета о прохождении учебной практики на итоговой конференции.*

По итогам выполнения каждого практического задания студентом-практикантом составляется **отчет о выполнении задания** в письменной форме, состоящий из титульного листа и текста отчета: цель работы, ход выполнения работы, вывод. Отчет должен отражать полученные практикантом организационно-технические знания и навыки. Он составляется на основании выполняемой работы, личных наблюдений и исследований. Отчет должен быть выполнен технически грамотно, иллюстрирован эскизами, схемами, фотографиями. Примерный объем отчета 5-6 страниц.

Отчет оформляется с помощью печатающих устройств на одной стороне листа бумаги формата А4. Размер шрифта 12-14 через 1-1,5 интервала. При написании текста следует оставлять поля слева - 30 мм, справа - 10 мм, сверху и снизу - 20 мм. Все страницы должны иметь сквозную нумерацию: первой страницей является титульный лист. На титульном листе номер не ставится. Номер страницы проставляется внизу по центру.

Отчет о выполнении задания проверяется преподавателем-руководителем практики.

По окончании практики студент предоставляет на кафедру **итоговый отчет о прохождении учебной практики** (далее - отчет), по содержанию включающий в себя результаты выполненных работ. Отчет обязательно должен содержать не только информацию о выполнении заданий программы практики, но и анализ этой информации, выводы и рекомендации, разработанные каждым студентом самостоятельно.

Отчет о практике является обязательным документом студентов-практикантов.

Оценка результатов по итогам учебной практики проводится на основании материалов отчета о практике, оформленного в соответствии с установленными требованиями. По форме он должен включать титульный лист и текст отчета. Титульный лист должен быть подписан руководителем практики и студентом-практикантом. Оформленный итоговый отчет должен быть сброшюрован в папку со скоросшивателем.

Текст отчета должен содержать:

1. содержание
2. описание целей прохождения учебной практики.
3. описание индивидуального задания (постановка целей выполнения).
4. ход выполнения индивидуальных заданий (пояснительный текст, скриншоты).
5. вывод по итогам выполнения индивидуальных заданий.

Отчёт может содержать приложения:

- материалы, собранные студентом в период прохождения практики (копии нормативно правовых и организационных документов, а также те документы, в составлении которых студент, принимал непосредственное участие в объёме, предусмотренном заданием);
- схемы, таблицы, аналитические расчёты, статистические данные, иллюстрации и т.п.

Отчет готовится в течение всей практики и проверяется преподавателем-руководителем практики до защиты отчета по практике. Оформленный отчет о практике, подлежит обязательной защите студентом в установленные сроки.

По итогам защиты отчета выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной практике по получению первичных профессиональных умений и навыков

7.1. 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

Выполнить следующие *практические задания*:

1. Изучить тему «Виды угроз информации», используя различные источники информации (библиотечный фонд, интернет ресурсы, лекционные материалы и т.п.). При изучении темы дать письменные ответы на представленные вопросы с указанием ссылки на источник заимствования.
   Вопросы:
   1. Что такое угроза безопасности информации.
   2. Приведите примеры организационных угроз.
   3. Приведите примеры технологических угроз.
   4. Какие каналы утечки информации существуют в компьютерных классах?

   Задание:

   Определите и классифицируйте угрозы безопасности вашего ПК.

Вид угрозы (ее описание)	Нарушение какого свойства информации несет представленная угроза (целостность, доступность, конфиденциальность)	Происхождение угрозы (случайное/преднамеренное)	Источник угрозы

2. Изучите тему «Вредоносное программное обеспечение».
   Вопросы:
   1. В чем состоит проблема вирусного заражения программ?
   2. Приведите классификацию вредоносного программного обеспечения.
   3. Опишите способы их обнаружения и наносимый ущерб?
   4. Какие вредоносные программные закладки кроме вирусов существуют?
   5. Какие существуют методы борьбы с компьютерными вирусами?

   Задание:

Раскройте сущность приведенного вируса:

Руткит	Boot – вирус	Макровирус	Полиморфный

3. Изучите тему «Антивирусные программы».
   Вопросы:
   1. Какие основные антивирусные программы вы знаете, кратко охарактеризуйте их. (не менее 6 программ).
   2. Каким образом происходит лечение зараженных дисков?
   3. Что такое программа – полифаг?
   4. Что такое программа - детектор?

   Задание:

   Дайте сравнительную характеристику следующих антивирусных программ:

	Dr.Web Antivirus	Avira Free Antivirus	AVG Anti-Virus Free	Avast! Free Antivirus
Анти – руткит				
Веб – антивирус				
Поиск и закрытие уязвимостей				

Проверка почтовых сообщений				
Сканирование до загрузки ОС				
Анти-баннер				
Отключение отслеживания действий в браузере				
Защита персональных данных				
Защита настроек антивируса паролем				
Использование облачных технологий				
Вывод				

4. Определение порядка допуска должностных лиц и граждан Российской Федерации к государственной тайне и заполнение форм учетной документации, необходимой для оформления такого допуска.
5. Определение общего порядка обращения с документами и другими материальными носителями информации, содержащими служебную информацию ограниченного распространения.
6. Структурная характеристика нормативно-правовых актов в области обеспечения защиты персональных данных.
7. Состав и назначение, порядок создания, утверждения и исполнения должностных инструкций. Составить штатное расписание сотрудников предприятия и утвердить должностные инструкции к нему.
8. Разработка пакета организационно-распорядительных документов для организации защиты конфиденциальной информации на предприятии.
9. Сравнительная характеристика антивирусных программ. Установка и настройка антивирусных программ: *Dr.Web, NOD 32*. Представить их сравнительный анализ в форме отчета и сделать вывод.

Наименование антивирусного ПО (версия) / Сравнительные характеристики		
1. Типы вирусов найденные ПО		
2. Стоимость ПО (от- до)		
3. Наличие сертификата ФСТЭК		
4. Скорость установки ПО		
5. Кол-во найденных вредоносных программ (из числа просканированных файлов)		
6. Время затраченное на поиск		

10. Сравнительный анализ программно-аппаратных средств защиты информации: *Аккорд, Аура, Соболь, КриптоПро, Аргус, Ручей-М, SecretNet, Dallas Lock, Acronis, XSpider, MaxPatrol, eToken, RuToken, VipNet CUSTOM.*
    Сравнительные характеристики: *Фирма производитель, тип продукта (программный, аппаратный и др.), уровень защиты по виду тайны (ГТ, КИ, ПДн, и др.), наличие сертификата ФСТЭК или ФСБ, стоимость (от-до)*
11. Установка и настройка программно-аппаратной системы защиты информации «Аккорд», «Аура», «Dallas Lock» и др.
12. Подготовка отчета о прохождении учебной практики.
13. Защита отчета.

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

Практическое задание / Компетенция	1.	2.	3.	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***
ОК-5				+	+		+	+					
ОК-6						+	+	+					
ОК-7				+			+			+		+	+
ОК-8	+	+	+				+			+		+	+

Практическое задание / Компетенция	1.	2.	3.	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***
ОК-9				+						+		+	+
ОК-11										+		+	+
ОК-12										+		+	+
ПК-1							+					+	
ПК-2	+	+	+	+			+						
ПК-3				+	+	+		+					
ПК-4				+			+					+	+
ПК-5					+		+	+		+	+		
ПК-8					+	+	+	+	+	+	+		
ПК-9					+			+	+				
ПК-10								+	+				
ПК-11									+	+	+		
ПК-12							+	+					
ПК-13	+						+	+					
ПК-14				+	+								
ПК-15			+		+					+	+		
ПК-16									+	+	+		
ПК-19	+	+	+				+			+		+	
ПК-20									+	+			
ПК-24	+	+	+	+	+	+		+				+	+
ПК-28				+	+			+	+				
ПК-29								+	+	+			
ПК-32										+	+		

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

По итогам выполнения каждого практического задания студентом-практикантом составляется **отчет о выполнении задания** в письменной форме, состоящий из титульного листа и текста отчета: цель работы, ход выполнения работы, вывод. Примерный объем отчета 4-8 страниц.

Каждое выполненное практическое задание оценивается «зачет/незачет» по следующим основным критериям:

1. Уровень выполнения задания: соответствует формированию закрепленной компетенции.

2. Полнота раскрытия темы задания, обоснованность выводов, предложений.

2. Качество оформления отчета.

3. Степень самостоятельности в работе: изложение, оригинальность составленных таблиц, схем и других материалов.

4. Научно-исследовательский подход, грамотность, стилистическая правильность текста.

При получении «зачета» за выполнение практического задания, закрепленная в соответствии с таблицей компетенция считается частично сформированной.

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

По итогам выполнения каждого практического задания студентом-практикантом составляется **отчет о выполнении задания** в письменной форме, состоящий из титульного листа и текста отчета: цель работы, ход выполнения работы, вывод. Примерный объем отчета 4-8 страниц.

Каждое выполненное практическое задание оценивается «зачет/незачет» по следующим основным критериям:

1. Уровень выполнения задания: соответствует формированию закрепленной компетенции.

2. Полнота раскрытия темы задания, обоснованность выводов, предложений.

2. Качество оформления отчета.

3. Степень самостоятельности в работе: изложение, оригинальность составленных таблиц, схем и других материалов.

4. Научно-исследовательский подход, грамотность, стилистическая правильность текста.

При получении «зачета» за выполнение практического задания, закрепленная в соответствии с таблицей компетенция считается частично сформированной.

Защита **итогового отчета о прохождении учебной практики** проводится в назначенное время и включает:

- предоставление письменного отчета о прохождении практики.
- краткое сообщение студента о результатах учебной практики, проведенных исследованиях и конкретных предложениях (3-5 минут).
- вопросы к студенту и ответы на них (3-5 минут).

По итогам защиты отчета выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно).

Критерии оценки:

"Отлично" оценивается работа студента, выполнившего весь объем работы, определенной программой практики, проявившего теоретическую подготовку и умелое применение полученных знаний в ходе практики, оформившего отчеты практики в соответствии со всеми требованиями; уверенно владеющего материалом при устной защите и правильно отвечающего на вопросы.

"Хорошо" - оценивается работа студента, который полностью выполнил программу практики, проявил самостоятельность, интерес к профессиональной деятельности, однако, при оформлении отчетов практики и (или) при ответах на вопросы допустил недочеты;

"Удовлетворительно" - оценивается работа студента, который выполнил программу практики, но при этом не проявил самостоятельности, допустил небрежность в формулировании выводов в отчете практики, не показал интереса к выполнению заданий практики, небрежно оформил отчеты практики, несвоевременно представил отчетные документы, допускал существенные недочеты при ответах на вопросы.

"Неудовлетворительно" - оценивается работа студента, не выполнившего программу практики, непредставившего отчет о практике или представившего отчет о практике, выполненный на крайне низком уровне, систематически непосещавшего занятий, не участвовшего в итоговой конференции по практике.

7.5. Показатели и критерии оценивания сформированности компетенций (на различных этапах их формирования), шкалы и процедуры оценивания.

Перечень компетенции	*Общее кол-во практических заданий для формируемых компетенций*	*Min кол-во заданий для выполнения*
ОК-5	*4*	*3*
ОК-6	*3*	*2*
ОК-7	*5*	*3*
ОК-8	*7*	*4*

ОК-9	*4*	*3*
ОК-11	*3*	*2*
ОК-12	*3*	*2*
ПК-1	*2*	*3*
ПК-2	*5*	*3*
ПК-3	*4*	*3*
ПК-4	*4*	*3*
ПК-5	*5*	*3*
ПК-8	*7*	*4*
ПК-9	*3*	*2*
ПК-10	*2*	*2*
ПК-11	*3*	*2*
ПК-12	*2*	*2*
ПК-13	*3*	*2*
ПК-14	*2*	*2*
ПК-15	*4*	*2*
ПК-16	*3*	*2*
ПК-19	*6*	*4*
ПК-20	*2*	*2*
ПК-24	*9*	*5*
ПК-28	*4*	*3*
ПК-29	*3*	*2*
ПК-32	*2*	*2*

8. Перечень учебной литературы и ресурсов сети "Интернет", необходимых для проведения учебной практики по получению первичных профессиональных умений и навыков

а) основная литература: (не старше 5 лет)

1. Носов Л.С., Биричевский А.Р. Техническая защита информации. Часть 1. Инженерно-техническая защита информации. Сыктывкар: издательство Сыктывкарского государственного университета, 2012. (электронный вариант)
2. Носов Л.С., Биричевский А.Р., Едомский Д.Н. Техническая защита информации. Часть 2. Технические средства защиты информации [Электронный ресурс] / Сыктывкар: ИПО СыктГУ, 2012.
3. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с.

б) дополнительная литература: (не старше 10 лет)

1. Артемов А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.
2. Сычев Ю.Н. Основы информационной безопасности: учебно-практическое пособие / Ю.Н. Сычев. - М.: Евразийский открытый институт, 2010. - 328 с.
3. Ярочкин В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. - 5-е изд. - М.: Академический проект, 2008. - 544 с.

Учебно-методические материалы

1. Учебно-методические материалы по программе «Аттестация объектов информатизации по требованиям безопасности информации» / ГНИИ ПТЗИ ФСТЭК России. Центр повышения квалификации специалистов по ТЗИ. (Диск CD-R)

2. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. / Утвержден Первым заместителем Председателя Гостехкомиссии России 08.11.2001.

Нормативно-правовые акты

1. Конституция РФ от 12.12.1993.
2. Трудовой кодекс РФ № 197 – ФЗ от 01.02.2002.
3. Гражданский кодекс Российской Федерации.
4. Уголовный кодекс российской федерации.
5. Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» принятый 27 июля 2006 года.
6. Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности"
7. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
8. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»
9. Постановление Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации»
10. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»
11. Постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»

в) Интернет-ресурсы

1. http://www.fstec.ru
2. http://www.ispdn.ru
3. http://www.rsoc.ru
4. http://www.itsec.ru
5. http://www.intuit.ru
6. http:/www.biblioclub.ru
7. http://www.CyberSecurity.ru

9. Перечень информационных технологий, используемых при проведении учебной практики по получению первичных профессиональных умений и навыков, включая перечень программного обеспечения и информационных справочных систем

Для проведения учебной практики, для выполнения целей и задач практики необходимо:
1. Справочно-правовая система КонсультатнтПлюс
2. Программное обеспечение:
- операционная система Windows 7,
- средства виртуализации VMware Player,
- пакет прикладных программ Microsoft Office,
- программно-аппаратная система защиты информации «Аккорд»,
- программно-аппаратная система защиты информации «Аура»,
- программно-аппаратная система защиты информации «Dallas Lock»,
- средство анализа защищенности сети Xspaider.

10. Описание материально-технической базы, необходимой для проведения учебной практики по получению первичных профессиональных умений и навыков.

Материально-техническое обеспечение учебной практики включает в себя:

1. аудиторию, оснащенную мультимедийными средствами (проектор, ноутбук, колонки)
2. технические средства:

- средства инженерно-технической защиты информации (генераторы шума, фильтры, средства выявления технических каналов утечки информации),
- средства оценки защищенности информации от утечки по техническим каналам: виброшумомер SVAN-959, генератор шума (в комплекте с акустическими и виброизлучателями), анализатор спектра Rohde&Schwarz FS300 с антенной АИ-5.0, набор тестов ПЭМИН, Селективные микровольтметры SMV-11 и SMV-8.5.

11. Иные сведения и материалы.

В целом в период прохождения учебной практики студент должен в обязательном порядке ознакомиться *со следующими вопросами*:

1. Правила техники безопасности и порядок организации труда на рабочих местах.
2. Порядок организации прохождения практики. Цель и задачи учебной практики.
3. Требования к оформлению отчетности и защиты отчетов по практике.
4. Основные обязанности должностных лиц подразделений по защите информации.
5. Требования к оформлению организационно-распорядительных документов.
6. Правовые и организационные основы защиты информации.
7. Особенности эксплуатации и состав технических, программных, аппаратных средств защиты информации.

Студент при прохождении учебной практики **обязан:**

- соблюдать правила охраны труда и техники безопасности;
- полностью выполнять задания, предусмотренные программой практики;
- эффективно использовать отведенное для практики время;
- качественно выполнять все практические задания;
- осуществлять сбор и анализ материалов, необходимых для подготовки отчета по практике;
- применять на практике полученные знания по изученным дисциплинам;
- представить руководителю практики письменный отчет о выполнении всех заданий и защитить его (в форме дифференцированного зачета).

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СЫКТЫВКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПИТИРИМА СОРОКИНА»
ИНСТИТУТ ТОЧНЫХ НАУК И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Отчет о выполнении задания №1

Виды угроз информации

Выполнил: студент 133 гр.
И.О. Фамилия

Сыктывкар 20__г.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СЫКТЫВКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ПИТИРИМА СОРОКИНА»
ИНСТИТУТ ТОЧНЫХ НАУК И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Отчет
о прохождении учебной практики

Направление подготовки

090900 Информационная безопасность
(бакалавриат)

Сроки практики_____

Выполнил:
Студент группы _____ _____ И.О. Фамилия
«____»__20__ г.

Проверил:
(Должность, ученная степень) _____ И.О. Фамилия
«___» _____20__ г.

Итоговая оценка по практике _____

Сыктывкар 20__г.