ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВПО УрГУПС)

Кафедра «Информационные технологии и защита информации»

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.А. Малыгин
«2» 11 2012 г.

Основная образовательная программа
«Информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Учебная практика», «Производственная практика»

Шифр дисциплины – ***090900.62***

Направление подготовки – ***Информационная безопасность***

Квалификация – ***бакалавр***

Форма обучения - ***очная***

Екатеринбург
2012

Рабочая программа дисциплин «Учебная практика», «Производственная практика» составлена в соответствии с основной образовательной программой подготовки бакалавров по направлению 090900.62 «Информационная безопасность».
Дисциплины «Учебная практика», «Производственная практика» базируются на основе ранее изученных дисциплин: «Техническая защита информации», «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности», «Информационные технологии», «Методология защиты информации», «Безопасность операционных систем», «Безопасность сетей ЭВМ», «Безопасность систем баз данных», «Теория информационной безопасности», «Защита и обработка конфиденциальных документов», «Комплексные системы защиты информации», «Защита информационных процессов в компьютерных системах».

Рабочая учебная программа обсуждена на заседании кафедры «Информационные технологии и защита информации»
19.04. 2012 протокол № 7.

Согласование:

Автор:
к-т тех. наук Т.Ю. Зырянова

Зав. кафедрой ИТиЗИ
д-р физ.-мат. наук., проф. Ю.И. Ялышев

Декан факультета ЭТФ
к-т физ.-мат. наук., доцент В.В. Башуров

Программа согласована:

Председатель учебно-методической комиссии факультета Н.Л. Ракина

Директор Екатеринбургского филиала
ФГУП «ЗащитаИнфоТранс»
Министерства транспорта
Российской Федерации С.Н Соловьев

Директор Екатеринбургского
НТЦ ФГУП «НЛП «Гамма» А.С. Худеньких

Учебная практика	
Курс	3
Семестр(ы)	6
Зачетные единицы	3
Диф. зачет	6 семестр
Объем	108 часов
Кол-во недель	2

Производственная практика	
Курс	4
Семестр(ы)	7, 8
Зачетные единицы	9
Диф. зачет	7, 8 семестр
Объем	324 часа
Кол-во недель	6

СОДЕРЖАНИЕ

1 Цели и виды практик

Производственное обучение студентов по направлению «Информационная безопасность» является составной частью образовательной программы высшего профессионального образования.

В соответствии с Федеральным государственным стандартом высшего профессионального образования по направлению подготовки «Информационная безопасность» определены следующие виды практик:

- практика для получения первичных профессиональных умений и навыков (учебная);
- практика (производственная) по направлению подготовки «Информационная безопасность».

Целью учебной практики студентов является изучение производственной структуры предприятия и приобретение опыта работы в трудовом коллективе.

Целью производственной практики студентов является закрепление и расширение теоретических знаний, полученных при изучении специальных дисциплин, овладение навыками по разработке организационных мероприятий, применению программных и технических средств защиты информации.

2 Задачи практик

Задачи учебной практики:

1. Ознакомление с организационной и информационной инфраструктурой предприятий – объектов практики.
2. Ознакомление с используемыми на объектах практики программными и техническими средствами защиты информации.

Задачи производственной практики

1. Приобретение практических навыков по организации защиты информации на объектах практики.
2. Ознакомление с используемыми на объектах практики программными и техническими средствами защиты информации.
3. Приобретение практических навыков по техобслуживанию, ремонту и монтажу оборудования защиты информации, применяемого на объекте практики.
4. Изучение графика технологического процесса на объектах практики.
5. Ознакомление с вопросами метрологии, стандартизации и оценки качества, а также с вопросами организации, планирования и управления предприятием.

3 Место практик в структуре ООП бакалавриата

Учебная практика базируется на освоении дисциплин:

Б3.Б.7 – Техническая защита информации;

Б3.Б.8 – Сети и системы передачи информации;

Б3.Б.9 – Организационное и правовое обеспечение информационной безопасности;

Б3.Б.15 – Информационные технологии;

Б3.В.ОД.1 – Методология защиты информации;

Б3.В.ОД.2 – Безопасность операционных систем;

Б3.В.ОД.3 – Безопасность сетей ЭВМ;

Б3.В.ОД.4 - Безопасность систем баз данных;

Б3.В.ОД.6 – Теория информационной безопасности.

Производственная практика базируется на освоении дисциплин:

Б3.Б.7 – Техническая защита информации;

Б3.Б.8 – Сети и системы передачи информации;

Б3.Б.9 – Организационное и правовое обеспечение информационной безопасности;

Б3.Б.15 – Информационные технологии;

Б3.В.ОД.1 – Методология защиты информации;

Б3.В.ОД.2 – Безопасность операционных систем;

Б3.В.ОД.3 – Безопасность сетей ЭВМ;

Б3.В.ОД.4 - Безопасность систем баз данных;

Б3.В.ОД.5 – Защита и обработка конфиденциальных документов;

Б3.В.ОД.6 – Теория информационной безопасности;

Б3.В.ДВ.5 – Комплексные системы защиты информации; Защита информационных процессов в компьютерных системах.

Для успешного прохождения учебной практики студент должен:

Знать: Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации. Эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы. Место и роль информационной безопасности в системе национальной безопасности Российской Федерации. Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы по техническому и экспортному контролю в данной области. Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в области сертификации средств защиты информации. Принципы и методы организационной защиты информации. Принципы построения информационных систем. Принципы организации информационных систем в соответствии с требованиями по защите информации. Назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ, основные понятия и методы математической логики и теории алгоритмов диспетчеризации, способы проверки операционных систем на безопасность использования различных программных и аппаратных средств. Основы администрирования вычислительных сетей. Системы управления базами данных.

Уметь: Анализировать и оценивать угрозы информационной безопасности объекта. Формулировать и настраивать политику безопасности распространения операционных систем, а также локальных вычислительных сетей, построенных на их основе. Пользоваться нормативными документами по защите информации. Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Использовать программные и аппаратных средства персонального компьютера. Использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав. Оценивать эффективность управленческих решений и анализировать экономические показатели

деятельности подразделений. Определять предельные параметры информационных потоков, обрабатываемых вычислительным комплексом; моделировать операции по распределению ресурсов между процессами, формулировать и настраивать политику безопасности распространенных операционных построенных на их основе вычислительных сетей, систем, а также локальных вычислительных сетей, построенных на их основе, проверять операционные системы на безопасность использования различных программных и аппаратных средств. Выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах.

Владеть: Методами формирования требований по защите информации. Навыками организации и обеспечения режима секретности. Навыками работы с нормативными правовыми актами. Навыками применения современных информационных технологий в профессиональной деятельности. Навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности. Навыками обоснования, выбора, реализации и контроля результатов управленческого решения. Методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации. Методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов. Методами анализа и формализации информационных процессов объекта и связей между ними.

Прохождение учебной практики необходимо как предшествующее для:
Прохождения производственной практики;
Итоговой государственной аттестации.

Для успешного прохождения производственной практики студент должен:

Знать: Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации. Эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы. Место и роль информационной безопасности в системе национальной безопасности Российской Федерации. Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы по техническому и экспортному контролю в данной области. Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны в области сертификации средств защиты информации. Принципы и методы организационной защиты информации. Принципы построения информационных систем. Принципы организации информационных систем в соответствии с требованиями по защите информации. Назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ, основные понятия и методы математической логики и теории алгоритмов диспетчеризации, способы проверки операционных систем на безопасность использования различных программных и аппаратных средств. Основы администрирования вычислительных сетей. Системы управления базами данных. Структуру систем документационного обеспечения. Принципы и методы

противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Уметь: Анализировать и оценивать угрозы информационной безопасности объекта. Формулировать и настраивать политику безопасности распространения операционных систем, а также локальных вычислительных сетей, построенных на их основе. Пользоваться нормативными документами по защите информации. Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Использовать программные и аппаратных средства персонального компьютера. Использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав. Оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделений. Определять предельные параметры информационных потоков, обрабатываемых вычислительным комплексом; моделировать операции по распределению ресурсов между процессами, формулировать и настраивать политику безопасности распространенных операционных построенных на их основе вычислительных сетей, систем, а также локальных вычислительных сетей, построенных на их основе, проверять операционные системы на безопасность использования различных программных и аппаратных средств. Выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах. Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Владеть: Методами формирования требований по защите информации. Навыками организации и обеспечения режима секретности. Навыками работы с нормативными правовыми актами. Навыками применения современных информационных технологий в профессиональной деятельности. Навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности. Навыками обоснования, выбора, реализации и контроля результатов управленческого решения. Методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации. Методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов. Методами анализа и формализации информационных процессов объекта и связей между ними.

Прохождение производственной практики необходимо как предшествующее для итоговой государственной аттестации.

4 Формы проведения практик

Учебная практика осуществляется форме лекций и экскурсий на предприятиях, выполнении обучающимися индивидуальных заданий.

Производственная практика основывается на выполнении обучающимися индивидуальных заданий на предприятиях и в организациях в области информационной безопасности.

5 Места и время проведения практик

Места проведения практик:

Екатеринбургский информационно-вычислительный центр – структурное подразделение Главного вычислительного центра – филиала ОАО «РЖД»;

Управление Федеральной службы по техническому и экспортному контролю по Уральскому Федеральному округу;

Екатеринбургский НТЦ ФГУП «НПП «Гамма»;

ЗАО «Производственная фирма «СКБ КОНТУР»;

ООО «ЦИНТУР»;

Научно-производственное предприятие «Специальные вычислительные комплексы».

Время проведения учебной практики: 2 недели в июле в соответствии с утвержденным графиком учебного процесса.

Время проведения производственной практики: 4 недели в начале 4-го курса и 2 недели перед выходом на государственную итоговую аттестацию в соответствии с утвержденным графиком учебного процесса.

6 Компетенции обучающегося, формируемые в результате прохождения практик

В результате прохождения учебной практики обучающийся должен приобрести следующие практические навыки, умения, универсальные и профессиональные компетенции:

способность 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);

способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

способность 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);

способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);

способность 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).

В результате прохождения производственной практики обучающийся должен приобрести следующие практические навыки, умения, универсальные и профессиональные компетенции:

способность к кооперации с коллегами, работе в коллективе (ОК-5);

способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

способность 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);

способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);

способностью администрировать подсистемы информационной безопасности объекта (ПК-10);

способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);

способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);

способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);

способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);

способность применять программные средства системного, прикладного и специального назначения (ПК-15);

способность использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);

способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);

способность применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);

способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24);

способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);

способностью участвовать в работах по реализации политики информационной безопасности (ПК-29);

способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32).

7 Организация практик

Практики студентов проводится в Екатеринбургском информационно-вычислительном центре – структурном подразделении Главного вычислительного центра – филиала ОАО «РЖД», Управлении Федеральной службы по техническому и экспортному контролю по Уральскому Федеральному округу, на предприятиях, осуществляющих деятельность в области защиты информации, а также предприятиях, заключивших договор на обучение студентов по целевым направлениям.

Направление студентов на практику производится в соответствии с договорами об организации и проведении производственной практики студентов.

Не позднее, чем за месяц до начала практики, формируется приказ, утверждаемый Проректором по учебной работе и связям с производством, в котором указываются объекты практики, ее продолжительность и назначаются руководители практики от университета, устанавливается график командировок руководителей на предприятия – базы производственной практики. Студенту на основании приказа выписывается путевка, являющаяся основанием для устройства на предприятии для прохождения практики, отчетным документом для кафедры и финансовым документом для последующих выплат в бухгалтерии.

Студенты, обучающиеся по целевому направлению от предприятий, направляются для прохождения практики на предприятия, заключившие договор на обучение данных студентов.

Направление студентов на практику может осуществляться в форме самостоятельного практикума: студент самостоятельно находит предприятие в качестве базы практики и информирует выпускающую кафедру о месте ее прохождения, предоставляя гарантийное письмо от предприятия.

Для студентов, обучающихся по целевому направлению от предприятия, в этом случае обязательно согласование с соответствующей службой.

Зачисление студентов на практику оформляется приказом по предприятию, где указываются рабочее место практиканта, в качестве кого он проходит практику и руководитель практики от предприятия, а также сроки ее окончания, которые соответствуют срокам производственной практики по учебному плану.

Перед началом практики (в первый день практики в соответствии с графиком учебного процесса) кафедра «Информационные технологии и защита информации» проводит организационное собрание студентов-практикантов и руководителей практики от университета для разъяснения целей, содержания и порядка прохождения практики, где студент получает выписку из приказа о направлении на практику, программу практики, путевку. На собрание приглашаются преподаватели-консультанты от кафедр «Экономика транспорта» и «Безопасность жизнедеятельности». Руководитель практики от университета и консультанты уточняют тему индивидуального задания и его содержание.

Студент обязан в двухнедельный срок после начала практики предоставить по факсу копию приказа о зачислении на предприятие для прохождения производственной практики. В течение практики студент готовит отчет по практике.

По возвращению в университет студент сдает ответственному за организацию практики на кафедре «Информационные технологии и защита информации» путевку с отзывом руководителя практики от производства и отметкой сроков прохождения практики, заверенными на производстве с приложением печатей предприятия. Руководителю практики от университета предъявляется отчет о практике для проверки. В начале следующего учебного семестра студентом сдается зачет, который принимается в университете по графику, устанавливаемому кафедрой. Неудовлетворительная оценка на зачете, отсутствие отчета или его оформление не в соответствии с тематикой индивидуального задания, а также самовольный уход с практики влечет повторное прохождение практики.

8 Обязанности сторон по организации и проведению практик

8.1 Обязанности руководителя практик от университета

Руководителями практики от университета назначаются преподаватели кафедры «Информационные технологии и защита информации» или лица, работающие на кафедре на условиях срочного трудового договора.

Руководитель практики от университета обеспечивает проведение всех организационных мероприятий перед выездом студентов на практику. До начала практики он обязан выявить наличие рабочих мест, должностей в соответствии с договором. Руководитель практики от вуза должен провести инструктаж студентов об их обязанностях и о порядке прохождения практики в строгом соответствии с программой.

До начала практики руководитель практики выдает индивидуальное задание, разрабатывает календарный график работы студентов с указанием рабочих мест, сроков и последовательности выполнения отдельных работ. Он осуществляет текущий контроль прохождения студентами практики и выполнение ими правил внутреннего распорядка, консультирует студентов по неясным вопросам, проверяет их отчеты по практике и совместно с руководителем от производства оценивает работу практикантов, представляет заведующему кафедрой письменный отчет о проведении практики, дает предложения и замечания по совершенствованию практической подготовки студентов.

8.2 Обязанности руководителя практик от производства

Общее руководство учебной и производственной практикой студентов осуществляет руководитель предприятия. Он подбирает специалистов в качестве руководителей практики. Руководителями назначаются опытные работники предприятия из числа инженерно-технических работников.

Руководители практики от производства несут персональную ответственность за выполнение программы и календарного графика практики студентов, соблюдение ими внутреннего распорядка предприятий, выполнение индивидуальных заданий. Они обязаны до начала практики организовать изучение студентами правил техники безопасности, а также провести инструктаж по ним.

Руководители от производства контролируют подготовку отчетов студентами-практикантами, в конце практики проверяют их, составляют на каждого студента производственную характеристику – отзыв руководителя практики от предприятия.

8.3 Обязанности студента-практиканта

Студент практикант обязан:

1. Прибыть на практику в установленные сроки, имея при себе:

– паспорт, студенческий билет, военный билет (приписное свидетельство), справку от нарколога, психиатра, справку о состоянии здоровья и прививках, медицинский полис, страховое свидетельство, копию ИНН – в случае установления этих требований предприятием;

– программу практики, путевку, а также документы, предусмотренные договором о практике.

2. Овладевать теоретическими знаниями и практическими навыками, в полном объеме в установленные сроки выполнить программу практики и индивидуальное задание.

3. Нести ответственность за выполненную работу и ее результаты.

4. Подчиняться действующим на предприятии (в учреждении, организации, фирме) правилам внутреннего трудового распорядка, правилам проживания в общежитии, соблюдать правила и нормы техники безопасности, производственной санитарии и противопожарной защиты.

5. Получить оценку работы и характеристику-отзыв у руководителя практики от предприятия, заверить их подписями и печатями.

7. Правильно оформлять на предприятии путевку с соблюдением сроков практики.

8. Своевременно сдать путевку, проездные и финансовые документы, копию приказа (распоряжения) руководителя предприятия о прохождении практики, отчет руководителю практики от кафедры.

9. Быть аттестованным по итогам практики в установленные приказом сроки.

9 Структура и содержание практик

Общая трудоемкость учебной практики составляет 3 зачетных единицы, 108 часов.

№ п/п	Разделы (этапы) практики	Виды учебной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Аудиторные занятия	Самостоятельная работа			
			Теоретические знания и экскурсии	Сбор материала	Выполнение индивидуального задания	
1	**2**	**3**	**4**	**5**	**6**	**7**
1	Инструктаж по технике безопасности	2	2			Экзамен на производстве

1	2	3	4	5	6	7
2	Организационные методы защиты информации на предприятии. Обзорные лекции	2	2			Устный опрос
3	Программные средства защиты информации на предприятии. Обзорные лекции	2	2			Устный опрос
4	Технические средства защиты информации на предприятии. Обзорные лекции	2	2			Устный опрос
5	Производственные экскурсии по рабочим местам предприятия		4			Посещение экскурсий
6	Сбор исходного материала			36		Проверка отчета
7	Выполнение индивидуального задания				52	Проверка отчета
	ИТОГО	8	12	36	52	**108**

Общая трудоемкость производственной практики составляет 9 зачетных единицы, 324 часа.

№ п/п	Разделы (этапы) практики	Виды учебной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Аудиторные занятия	Самостоятельная работа			
			Теоретические знания и экскурсии	Сбор материала	Выполнение индивидуального задания	
1	**2**	**3**	**4**	**5**	**6**	**7**
1	Инструктаж по технике безопасности	2	2			Экзамен на производстве
2	Комплексные системы защиты информации на предприятии. Обзорные лекции	6	6			Устный опрос
5	Производственные экскурсии по рабочим местам предприятия		10			Посещение экскурсий
6	Сбор исходного материала			154		Проверка отчета
7	Выполнение индивидуального задания				144	Проверка отчета
	ИТОГО	8	18	154	144	**324**

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

Теоретические занятия на объекте практики проводятся в минимально необходимом объеме с учетом особенностей объекта – не более четырех часов в неделю.

К чтению лекций и проведению бесед привлекаются руководители и ведущие специалисты предприятий.

Если практика проходит на конкретных рабочих местах, то предусматриваются производственные экскурсии по другим рабочим местам предприятия.

Индивидуальные задания выдаются в дополнение и развитие программы практики. Они могут быть связаны с научно-исследовательской работой кафедры, с темами дипломных проектов.

11 Учебно-методическое обеспечение самостоятельной работы студентов на практике

Контрольные вопросы, подлежащие изучению на объекте учебной практики

Организационные методы защиты информации на предприятии

1. Понятие концепции информационной безопасности.
2. Государственная система защиты информации: структура государственной системы защиты информации; основные организационно-технические мероприятия по защите информации; организация работ по защите информации на предприятии; организация защиты информации в системах и средствах информатизации и связи; контроль состояния защиты информации; финансирование мероприятий по защите информации.
3. Организационные мероприятия по защите информации: основные задачи службы безопасности; план мероприятий по защите информации предприятия; организационно-правовая структура защиты информации; стратегическая направленность защиты информации; типовой перечень задач службы безопасности; организационно-правовой статус службы безопасности; организационно технические и режимные меры (административные, организационно режимные); избирательная политика безопасности; организационно технические мероприятия.
4. Силы, обеспечивающие безопасность (закон Российской Федерации «О безопасности»).
5. Организация доступа, допуска (предоставление, основание отказа, формы допуска).
6. Аттестация объектов информатизации: органы аттестации - структура, функции; цель проведения аттестационных работ; виды объектов информатизации, подлежащих аттестации в обязательном порядке; исходные данные по аттестуемому объекту; методика проведения испытаний
7. Система лицензирования. Организационная структура, функции.
8. Система государственных нормативных актов, стандартов, руководящих документов и требований защиты информации от несанкционированного доступа: порядок приемки и сертификации СВТ; порядок организации и проведения разработок системы защиты информации в ведомствах и на отдельных предприятиях; порядок контроля эффективности защиты информации
9. Организация охраны предприятия. Организация внутриобъектового и пропускного режимов на предприятиях.
10. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.
11. Защита информации при публикаторской и рекламной деятельности.

Программные средства защиты информации на предприятии

1. Анализ стандартов и рекомендаций с практической точки зрения. Распространение подхода «клиент-сервер» на информационную безопасность. Наиболее распространенные угрозы информационной безопасности. Практический подход к созданию и поддержанию информационной безопасности на предприятиях различных форм собственности затрагивающие вышеописанные проблемы.
2. Политика безопасности. Пример составления политики безопасности для локальной вычислительной сети предприятия. Программа безопасности - управленческий

аспект. Управление рисками. Безопасность в жизненном цикле системы. Практический подход к созданию политики безопасности на предприятиях различных форм собственности, с примерами, затрагивающими управленческий аспект, управления рисками.

3. Управление персоналом. Физическая защита. Поддержание работоспособности. Реакция на нарушение режима безопасности. Планирование восстановительных работ. Практический подход к проблемам связанным с управлением персоналом, физической защитой программно-аппаратных комплексов и поддержание их работоспособности, а также реакции обслуживающего персонала на нарушение режима безопасности а планированию восстановительных работ.

4. Обзор наиболее распространённых методов «взлома». Комплексный поиск возможных методов доступа. Терминалы защищённой информационной среды. Получение пароля на основе ошибок администратора и пользователей. Получение пароля на основе ошибок в реализации. Социальная психология и социальный инжиниринг, иные способы получения паролей. Наиболее распространенные методы «взлома», различные способы получения пароля пользователя.

5. Атакуемые сетевые компоненты. Сервера. Рабочие станции. Среда передачи информации. Атакуемые сетевые компоненты. Узлы коммутации сетей. Уровни сетевых атак согласно модели OSI. Классификация атак. Методики атак и способы защиты от них на вышеуказанные компоненты информационной системы.

6. Обзор современного программного обеспечения. Операционные системы. Прикладные программы. Ошибки разработки, приводящие к возможности атак на информацию. Основные положения по разработке программного обеспечения. Ошибки в реализации механизмов защиты при разработке общесистемного и прикладного программного обеспечения.

7. Основные направления защиты информации. Системы управления доступом. Биометрические системы, электронные ключи. Системы учёта рабочего времени. Сетевая безопасность. Комплексный анализ уязвимостей и обнаружение атак. Межсетевые экраны. Адаптивная защита. Защита программного обеспечения (запутывающие преобразования, маскировка, криптография, стеганография). Цифровая подпись, сервера авторизации. Вирусы. Антивирусное программное обеспечение. Существующие механизмы защиты информации и перспективные наработки вышеупомянутых компонентов.

8. Использование источников бесперебойного питания. Повышение отказоустойчивости дисков с помощью RAID-массивов. Грозозащита. Системы непрерывной готовности. Кластерные системы. Повышение надежности хранения баз данных. Системы энергобезопасности, а так же системы надежного резервирования критичных данных.

Технические средства защиты информации на предприятии

1. Особенности информации как объекта защиты. Основные свойства информации как предмета защиты. Ценность информации. Нейтральная информация, вредная, полезная информация, информация как товар. Виды защищаемой информации. Семантическая информация. Признаковая информация.

2. Демаскирующие признаки объекта защиты. Признаки позволяющие отличить один объект от другого. Классификация демаскирующих признаков. Демаскирующие признаки характеристик объекта защиты. Видовые демаскирующие признаки. Демаскирующие признаки сигналов. Демаскирующие признаки веществ.

3. Источники и носители информации. Виды источников и носителей информации. Основные источники информации. Основные виды носителей информации. Принципы записи и съема информации с носителя. Источники сигналов. Источники функциональных сигналов. Побочные излучения и наводки. Акустоэлектрические преобразователи: индуктивные, емкостные, пьезоэлектрические. Опасные поля.

4. Угрозы безопасности информации. Виды угроз безопасности информации, защищаемой техническими средствами. Случайные и преднамеренные угрозы. Оценка величины угрозы.

5. Органы добывания информации. Основные сферы интересов деятельности разведки государства. Задачи органов коммерческой разведки, их состав и возможности. Виды технической разведки. Принципы добывания информации. Технология добывания информации. Добывания информации без физического проникновения в контролируемую зону. Показатели эффективности добывания информации.

6. Технические каналы утечки информации (ТКУИ). Характеристики ТКУИ. Классификация и структура ТКУИ. Оптический канал утечки информации. Радиоэлектронный канал утечки информации. Акустический канал утечки информации. Материально-вещественный канал утечки информации.

7. Задачи, принципы и основные методы защиты информации техническими средствами. Роль и место технических средств в организации режима охраны. Способы и средства инженерной защиты и технической охраны объектов. Подсистема инженерной защиты. Средства нейтрализации угроз. Способы и средства противодействия наблюдению, подслушиванию, утечки информации через закладные устройства, побочные излучения и наводки.

8. Основные составляющие систем технических средств охраны. Приборы и системы сбора и обработки информации. Датчики охранной, пожарной и тревожной сигнализации. Современные системы управления контролем доступа. Средства управления системой охраны. Подсистема наблюдения. Интегрированные системы безопасности.

Контрольные вопросы, подлежащие изучению на объекте производственной практики

1. Модели комплексных систем защиты информации. Модель, основанная на множествах объектов защиты, угроз и средств защиты. Модель, основанная на множествах основ, направлений и действии по защите информации. Модель стандарта ГОСТ Р ИСО/МЭК 15408.

2. Стандартизация комплексных систем защиты информации. ГОСТ Р ИСО/МЭК 15408–2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Международный стандарт ISO/IEC 27002 «Информационные технологии – Практические правила управления информационной безопасностью».

3. Нормативно-правовые основы защиты информации.

4. Политика безопасности. Определения, составляющие, этапы разработки.

5. Основные понятия управления информационными рисками. Понятия ущерба, риска, анализа рисков, управление рисками и их соотношение. Классификация видов информационного ущерба и информационного риска, методов управления информационными рисками.

6. Инструментальные методики управления информационными рисками. CRAMM, RiskWatch, COBRA.

7. Статистические методики управления информационными рисками. Основы статистического анализа данных. Методы корреляционно-регрессионного анализа и анализа временных рядов, их применение к прогнозированию информационного риска.

8. Сравнительный анализ методик управления информационными рисками.

9. Программно-техническая составляющая комплексной системы защиты информации.

10. Экономическая составляющая комплексной системы защиты информации. Методика оценки затрат на защиту информации.

11. Ознакомление с практическими особенностями управления информационными рисками на предприятии.

12. Компонент системы защиты информации ViPNet [Клиент]. Инсталляция ПО ViPNet [Клиент]; изучение структуры каталога установки ПО ViPNet [Клиент]; изменение ключевой информации без переинсталляции ПО; смена режимов работы программы

Монитор; изучение настроек программы Монитор; изучение настроек параметров безопасности в Мониторе и Деловой почте; изучение работы с пользователями защищенной сети в Мониторе; изучение настроек работы через межсетевой экран; изучение работы с незащищенными компьютерами; изучение работы с фильтрами; изучение журналов блокированных и IP-пакетов и их настроек; определение URL или IP-адреса; смена пользователя в Мониторе и Деловой почте; настройка псевдонимов; работа с паролем администратора абонентского пункта; настройки MFTP; обеспечение работы по Dial-Up; журнал конвертов MFTP; очередь конвертов MFTP; формирование нового письма, отсылка одному или нескольким адресатам; использование ЭЦП; использование прикладного шифрования писем; флаги упаковки, отправки, доставки и прочтения писем в Деловой почте; изучение свойств письма; запуск внешних программ в Деловой почте; настройка автопроцессинга; путь письма при его удалении в Деловой почте; работа с Деловой почтой на абонентском пункте, где зарегистрировано несколько коллективов; переинсталляция ПО ViPNet [Клиент].

13. Компонент системы защиты информации ViPNet [Координатор]. Формирование виртуальной защищенной сети; развертывание виртуальной защищенной сети; настройка сетевых узлов для совместной работы.

12 Формы промежуточной аттестации (по итогам практики)

По итогам учебной практики - составление и защита отчета, дифференцированный зачет в 6-м семестре.

По итогам производственной практики - составление и защита отчетов, дифференцированный зачет в 7 семестре, дифференцированный зачет в 8 семестре.

13 Учебно-методическое и информационное обеспечение практик

а) основная литература:

1. Романов, О.А. Организационное обеспечение информационной безопасности: Учебник для студ. высш. учеб. заведений / О.А. Романов, С.А. Бабин, С.Г. Жданов. - М.: Издательский центр «Академия», 2008. - 192 с.
2. Корнеев, И.К. Защита информации в офисе / И.К. Корнеев, И.А. Степанова. - М.: ТК ВЕЛБИ, 2008. - 336 с.
3. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - М.: Горячая линия –Телеком, 2009.- 552 с.
4. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. Учебное пособие для студентов высших учебных заведений / В.Ф. Шаньгин. - М.: ДМК Пресс, 2008.
5. Духан, Е.И. Применение программно-аппаратных средств защиты компьютерной информации / Духан Е.И., Синадский Н.И., Хорьков Д.А. - Екатеринбург: УГТУ-УПИ, 2008. - 182 с.
6. Разрушающие программные воздействия: учеб.-метод. пособие / под ред. М.А. Иванова. - М.: НИЯУ МИФИ, 2011. — 328 с.
7. Будник, А.В. Физические и аппаратные средства защиты информации и их проектирование / А.В. Будник, В.М. Логин. – Минск: БГУИР, 2011. – 36 с.

8. Торокин, А.А. Инженерно-техническая защита информации (учеб.пособие для студентов, обучающихся по специальностям в обл. информ.безопасности) / А.А. Торокин.- М.: Изд-о Гелиос АРВ, 2008.-960 с.
9. Зайцев, А.П. Технические средства и методы защиты информации / под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО «Издательство Машиностроение», 2009 - 508 с.
10. Домарев, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2008.

б) дополнительная литература:

1. Закон Российской Федерации «О безопасности», № 2446-1 от 1.04.1994, (с изменениями № 103-ФЗ от 26.06.2008).

2. Закон Российской Федерации «О государственной тайне», № 5485-1 от 21.07.93, (с изменениями № 314-О от 10.11.2002).

3. Федеральный закон «Об информации, информационных технологиях и защите информации», №149-ФЗ от 27.07.2006 г.

4. Федеральный закон «О персональных данных» № 152-ФЗ от 27 июля 2006. (с изменениями № 261-ФЗ от 25.07.2011).

5. Указы Президента РФ:

- Указ Президента РФ «Об основах государственной политики в сфере информатизации», №170 от 20.01.94;

- «Перечень сведений, отнесенных к государственной тайне», от 18.05.2009 N 565, от 10.06.2009 N 640, от 30.09.2009 N 1088;

- «Перечень сведений конфиденциального характера», №188 от 6.03.97.

6. Ведомственные нормативные акты и Руководящие документы:

- «Положение о государственном лицензировании деятельности в области защиты информации», решение Гостехкомиссии и ФАПСИ №10 от 27.04.94 (с изменениями и дополнениями от 24 июня 1997г. №60);

- «Положение по аттестации объектов информатизации по требованиям безопасности информации», Гостехкомиссия России, от 24.11.1994;

- Приказ ФСТЭК России «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» от 5.02.2010 N 58.

- Методический документ «Методические рекомендации по технической защите конфиденциальной информации, составляющей коммерческую тайну», ФСТЭК России, 2007 г.(для служебного пользования).

7. Доктрина информационной безопасности Российской Федерации (Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895).

в) программное обеспечение и Интернет-ресурсы:

1. Материалы Интернет-сайтов:
   - CIT-Forum (www.citforum.ru)
   - информационный бюллетень «JetInfo On-line» (www.jetinfo.ru)
   - журналы «Открытые системы» (www.osp.ru)
   - журнал сетевых решений «LAN» (www.osp.ru/lan)
   - журнал «Сети» (www.osp.ru/nets)
   - журнал «Мир ПК» (www.osp.ru/pcworld)
   - журнал «IT Manager» (itm.finestreet.ru)
   - журнал «Экспресс-Электроника» (electronica.finestreet.ru)
   - журнал «Защита информации. Конфидент» (www.confident.ru/magazine)
2. Публикации на Интернет-сайтах фирм-производителей и интеграторов средств и систем защиты информации:

«Информзащита» (www.infosec.ru)
«Positive Technology» (www.ptsecurity.ru)
«Biolink» (www.biolink.ru)
«Cisco Systems» (www.cisco.com)
«Элвис-плюс» (www.elvis.ru)

14 Требования к составлению отчета по практике

Отчет по практике является основным документом, характеризующим работу студента во время практики. Объем отчета должен быть от 15 до 20 страниц печатного текста.

Содержание отчета по практике определяется: современным состоянием выбранного направления исследований; доступными литературными источниками; собранным для выполнения работ фактическим материалом.

Отчет по практике имеет следующую структуру:

1. титульный лист;
2. отзыв руководителя от предприятия;
3. оглавление;
4. введение;
5. описание предприятия – места практики;
6. теоретическая часть;
7. практическая часть;
8. выводы;
9. список использованной литературы;
10. приложения.

На титульном листе отчета указывается министерства, наименование вуза, факультета, кафедры, наименование практики, место ее проведения, фамилия, имя, отчество студента, индекс группы, фамилии руководителей практики от университета и предприятия и год составления отчета.

За титульным листом в отчете помещается отзыв руководителя от предприятия, заверенный печатью, затем оглавление.

Во введении дается обоснование темы работы, определяется ее практическая и/или теоретическая значимость для специальности, формулируются цели и задачи практической работы, а также приводится ее краткая аннотация (количество страниц, рисунков, таблиц, приложений, литературных источников).

В отчете обязательно должен быть раздел «Выводы», который содержит собственные суждения студента об организации практики, результатах решения поставленных перед ним задач, а также предложения по внедрению новых технологических средств. Это должно быть сделано на основе методологии проектирования, внедрения и эксплуатации систем защиты информации с оценкой их научно-технического уровня, замеченных недостатков и конкретных предложений по их устранению.

Описания должны быть сжатыми, ясными и сопровождаться численными данными, эскизами, схемами, графиками и чертежами.

Приложения оформляются как продолжение отчета. В приложениях помещаются чертежи, технологические карты и другие производственные материалы. Приложения нумеруют арабскими цифрами, а ниже слова «Приложение», расположенного справа, помещают название приложения, которое именуют, как и заглавие раздела, и приводят в оглавлении.

15 Материально-техническое обеспечение практик

Лаборатории, специально оборудованные кабинеты, измерительные и вычислительные комплексы, имеющиеся в распоряжении баз практики.

16 ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Уральский государственный университет путей сообщения»
(ФГБОУ ВПО УрГУПС)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ
На 20__20__учебный год.

По **Производственной (технологической) практике**, для направления бакалавриата 090900.62 «Информационная безопасность»

Основание:_____
_____
_____

В рабочую программу вносятся следующие изменения:
_____
_____
_____
_____
_____
_____
_____

Дополнения и изменения внесены на заседании кафедры_____
_____протокол №_____от_____20__г.

Автор рабочей программы_____
(Ф.И.О., подпись)
Зав. кафедрой _____
(Ф.И.О., подпись)
Декан факультета_____