Аннотация
программы учебной практики
Б2.У Учебная практика: практика по получению первичных профессиональных умений и навыков
направление подготовки
10.03.01 Информационная безопасность
образовательная программа
«Комплексная защита объектов информатизации»
Уровень образования
бакалавриат
Форма обучения
очная, очно-заочная

Цели и задачи практики	**Цель:** закрепление и углубление теоретической подготовки обучающегося, совершенствование качества профессиональной подготовки, приобретение им практических навыков и компетенций, формирование первичных профессиональных умений и навыков исследования и формализации прикладных задач по защите информации. **Задачи:** - - применение полученных знаний по профильным дисциплинам; - получение студентами первичных сведений по обеспечению комплексной защиты информации в различных типах организаций; - знакомство с правовым регулированием обеспечения информационной безопасности; - знакомство со специальным программным обеспечением и оборудованием для решения поставленной задачи по анализу защищенности объекта информатизации; - совершенствование навыков решения информационных задач на конкретном рабочем месте.
Способ и форма(ы) проведения практики	Учебная практика может проходить: в государственных, коммерческих и некоммерческих организациях; информационных подразделениях предприятий различных сфер деятельности, а так же научно-производственных организациях. Способы проведения учебной практики: стационарная; выездная. Форма проведения практики: дискретно.
Общая трудоемкость практики	В соответствии с учебным планом учебная практика по очной форме обучения проводится на 2 курсе в 4 семестре, а по очно-заочной форме обучения на 3 курсе в 6 семестре. Продолжительность практики составляет 2 недели. Общая трудоемкость учебной практики составляет 3 зачетных единиц, 108 часов.
Требования к результатам прохождения практики	
способностью понимать социальную значимость своей	**Знать:** основы требования к профессиональной деятельности специалиста в области защиты

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);	информации; основы информационной безопасности; нормы взаимоотношения в коллективе; **Уметь:** работать с различными программно-аппаратными средствами защиты информации; соблюдать нормы профессиональной этики; **Владеть:** основными трудовыми функциями специалиста по защите информации, специфику работы на данном предприятии; навыками профессионального общения
способностью к самоорганизации и самообразованию (ОК-8);	**Знать:** методы и средства, необходимые для самостоятельного выполнения заданий практики; состав отчетных документов и способы их подготовки; самостоятельно выбрать применяемые ИТ инструменты; **Уметь:** самостоятельно составить индивидуальный план своей деятельности на практике; подготовить письменный отчет о прохождении практики и представить его в Институт для защиты в установленные сроки; **Владеть:** навыками самостоятельного сбора необходимой информации для написания отчета по практике; навыками представления результатов проведенной работы в рамках практики; навыками составления отчета о проведенных работах в рамках практики.
способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);	**Знать:** организационную и производственную структуру предприятия; методы и технологии обработки информации; **Уметь:** анализировать организационную и производственную структуру предприятия; применять информационные технологии для поиска и обработки информации; **Владеть:** методами анализа структуры и содержания информационных процессов на предприятии; навыками решения информационных задач на конкретном рабочем месте.
способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);	**Знать:** основные нормативные документы и источники по угрозам информационной безопасности; **Уметь:** составлять обзор источников по вопросам обеспечения информационной безопасности **Владеть:** навыками подбора, изучения и обобщения нормативных правовых актов по вопросам обеспечения информационной безопасности, в том числе выбранного предприятия.;
способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10).	**Знать:** методы защиты информации и стандарты в области информационной безопасности; **Уметь:** выявлять источники угроз информационной безопасности предприятия; анализировать применяемые соответствующие методы и средства информационной безопасности; **Владеть:** навыками выявления источников угроз

	информационной безопасности; навыками работы со специальным программным обеспечением и оборудованием для решения поставленной задачи по анализу защищенности объекта информатизации
Содержание практики	Требуемые компетенции формируются при выполнении следующих заданий по учебной практике. **Подготовительный этап** Формулирование конкретных задач практической деятельности студентов, доведение формы и содержания отчетной документации (ОК-5, ОК-8, ОПК-4); **Основной этап** 1. Проанализировать организационную и производственную структуру организации, изучить нормативные акты (ОК-5, ОПК-4, ОПК-5); 2. Выявить источники угроз информационной безопасности. Результаты оформить в виде таблицы (ОК-5, ОК-8, ОПК-4, ПК-10); 3. Предложить идеи по совершенствованию информационного обеспечения структурного подразделения, организации и методов защиты информации с учетом соответствия требованиям стандартов в области информационной безопасности (ОК-5, ОК-8, ОПК-4, ПК-10); **Завершающий этап** Предоставить отчетные документы по итогам прохождение практики (ОК-5, ОК-8, ОПК-5): а) характеристику с места практики; б) отчет о прохождении практики; в) дневник практики.
Форма отчетности по практике	Отчет о прохождение практики

Аннотация
программы производственной практики
Б2.П Производственная практика: проектно-технологическая практика
направление подготовки
10.03.01 Информационная безопасность
образовательная программа
«Комплексная защита объектов информатизации»
Уровень образования
бакалавриат
Форма обучения
очная, очно-заочная

Цели и задачи практики	**Цель:** закрепление и углубление теоретических знаний по информационной безопасности и защите информации, программно-техническим, организационным и правовым методам обеспечения информационной безопасности, приобретение практических профессиональных навыков и формирование

	компетенций, опыта самостоятельной профессиональной деятельности. **Задачи:** - изучение структуры предприятия и действующей на нем системы управления; - изучение информационной структуры предприятия, информационных технологий, используемых на предприятии; - изучение перспективных разработок на предприятии; - закрепление знаний, полученных в процессе обучения, адаптация к рынку труда; - совершенствование навыков сбора, систематизации и анализа информации, необходимой для решения практических задач в сфере информационной безопасности; - приобретение навыков профессиональной работы и решения практических задач в сфере информационной безопасности.
Способ и форма(ы) проведения практики	Производственная практика может проходить: в государственных, коммерческих и некоммерческих организациях; информационных подразделениях предприятий различных сфер деятельности, а так же научно-производственных организациях. Способы проведения производственной практики: стационарная; выездная. Форма проведения практики: дискретно.
Общая трудоемкость практики	В соответствии с учебным планом производственная практика по очной форме обучения проводится на 3 курсе в 6 семестре, а по очно-заочной форме обучения на 4 курсе в 8 семестре. Продолжительность практики составляет 2 недели. Общая трудоемкость производственной практики составляет 3 зачетных единиц, 108 часов.
Требования к результатам прохождения практики	
способность 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)	**Знать:** основные требования к профессиональной деятельности специалиста в области защиты информации; нормы профессиональной этики; **Уметь:** работать с различными программно-аппаратными средствами защиты информации; соблюдать нормы профессиональной этики; **Владеть:** основными трудовыми функциями специалиста по защите информации, специфику работы на данном предприятии; навыками профессионального общения.
способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6)	**Знать:** основы взаимоотношений в коллективе; правила внутреннего распорядка организации; **Уметь:** выполнять возложенные функции специалиста по защите информации в коллективе; соблюдать правила и нормы охраны труда, техники

	безопасности, пожарной безопасности, правила внутреннего распорядка организации; **Владеть:** методами работы на конкретном рабочем месте; навыками проведения совместных работ и экспериментов в коллективе.
способностью к самоорганизации и самообразованию (ОК-8)	**Знать:** все задания, предусмотренные программой практики, и сроки их выполнения; методы и средства, необходимые для самостоятельного выполнения заданий практики; состав отчетных документов и способы их подготовки; **Уметь:** самостоятельно составить индивидуальный план своей деятельности на практике; подготовить письменный отчет о прохождении практики и представить его в Институт для защиты в установленные сроки. **Владеть:** навыками самостоятельного сбора и анализа исходных данных для проектирования систем защиты информации; навыками составления отчета о проведенных работах в рамках практики.
способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	**Знать:** необходимый математический аппарат для проведения проектных расчетов системы обеспечения информационной безопасности предприятия; **Уметь:** использовать математический аппарат для проектирования системы защиты информации; **Владеть:** навыками применения соответствующего математического аппарата для проектирования системы защиты информации.
способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	**Знать:** положения электротехники, электроники и схемотехники, которые используются в устройствах защиты информации; **Уметь:** применять основные положения электротехники, электроники и схемотехники для анализа функционирования технических средств защиты информации; **Владеть:** навыками использования электротехники, электроники и схемотехники при эксплуатации технических средств защиты информации.
способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);	**Знать:** типовые структуры предприятия, связи и автоматизации объектов информатизации, оснащенность техническими средствами; **Уметь:** проводить анализ структуры предприятия, средств и объектов автоматизации и информатизации, оснащенность техническими средствами; применять информационные технологии для поиска и обработки информации; **Владеть:** методами анализа структуры предприятия, автоматизации объектов информатизации, оснащенность техническими средствами; навыками построения ИТ инфраструктуры предприятия.
способностью использовать нормативные правовые акты в	**Знать:** нормативные правовые акты по вопросам информационной безопасности, в том числе выбранного

профессиональной деятельности (ОПК-5);	предприятия; **Уметь:** использовать нормативные материалы и стандарты в обосновании предложений по совершенствованию информационной безопасности предприятия; **Владеть:** нормативными правовыми актами по защите информации данного предприятия.
способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);	**Знать:** методы выявления угроз информационной безопасности; способы защиты от угроз информационной безопасности; **Уметь:** выявлять проблемы в организации информационной безопасности предприятия; применять средства и способы защиты информации; **Владеть:** методами выявления угроз информационной безопасности; навыками поиска инновационных способов защиты от угроз информационной безопасности.
способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	**Знать:** построение и функционирование программных, программно-аппаратных и технических средств защиты информации; **Уметь:** провести сравнительный анализ подсистем (программных, аппаратных, технических средств защиты информации) по показателям информационной безопасности предприятия. **Владеть:** навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);	**Знать:** программные и аппаратные средства защиты информации; **Уметь:** использовать необходимые программные и аппаратные средства для защиты информации на предприятии; **Владеть:** навыками настройки и эксплуатации программно-аппаратных средств защиты информации.
способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);	**Знать:** администрирование операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основных протоколов компьютерных сетей, подсистем информационной безопасности объекта защиты; **Уметь:** Работать с различными операционными системами, системами управления базами данных, в локальных и глобальных компьютерных сетях, с подсистемами информационной безопасности объекта защиты **Владеть:** навыками построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основных протоколов компьютерных сетей, подсистем информационной безопасности объекта защиты;
способностью принимать	**Знать:** порядок и регламент аттестации объекта

участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	информатизации по требованиям безопасности информации; **Уметь:** готовить документы к аттестации объекта информатизации по требованиям безопасности информации; **Владеть:** навыками сопровождения аттестации объекта информатизации по требованиям безопасности информации.
способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	**Знать:** правила проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; **Уметь:** проводить проверку работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; **Владеть:** навыками установки, настройки, эксплуатации и поддержания в работоспособном состоянии компонентов системы обеспечения информационной учетом установленных требований;
способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);	**Знать:** методы анализа исходных данных для разработки проекта совершенствования информационной безопасности предприятия; **Уметь:** провести технико-экономическое обоснование проекта по совершенствованию информационной безопасности предприятия; **Владеть:** методами составления технико-экономического обоснования проекта по совершенствованию информационной безопасности предприятия.
способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);	**Знать:** технологию подготовки технической документации по информационной безопасности предприятия; **Уметь:** оформить техническую документацию ; **Владеть:** составлением рабочей документации по информационной безопасности предприятия.
способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);	**Знать:** способы защиты от угроз информационной безопасности, стандарты безопасности в информационных системах; **Уметь:** проводить анализ информационной безопасности деятельности предприятия с учетом новейших нормативных материалов по вопросам информационной безопасности и в соответствии с требованиями стандартов; **Владеть:** методами анализа информационной безопасности объектов и систем в соответствии с требованиями стандартов.
способностью принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать:** методы проведения экспериментов по защите информации, подбору способов и средств защиты информации, определение достоверности проводимых экспериментов; **Уметь:** провести эксперимент по заданной тематике, в

(ПК-12)	том числе по подбору способов и средств защиты информации на предприятии; **Владеть:** методами проведения эксперимента по подбору способов и средств защиты информации на предприятии, обработку, оценку погрешности и достоверности результатов.
способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)	**Знать:** принципы организации и методы управления малым коллективом исполнителей; **Уметь:** распределять задачи между сотрудниками малого трудового коллектива по защите информации, установке и эксплуатации программно-аппаратных средств; **Владеть:** методами и средствами организации работ внутри малого трудового коллектива
Содержание практики	Требуемые компетенции формируются при выполнении следующих заданий по производственной практике. **Подготовительный этап** Формулирование конкретных задач практической деятельности студентов, доведение формы и содержания отчетной документации (ОК-5, ОК-8, ОПК-4). **Основной этап** 1. Провести анализ предприятия (отдела) по предложенным в задании характеристикам (ОК-6, ОПК-4, ОПК-5, ПК-1, ПК-2, ПК-3, ПК-6, ПК-8); 2. Провести сравнительный анализ подсистем (программных, аппаратных, технических средств защиты информации) по показателям информационной безопасности (ОПК-7, ПК-1, ПК-2, ПК-3, ПК-5,ПК-10); 3. Провести поиск оптимальных путей и инструментов решения для проектирования систем защиты информации (ПК-5, ПК-10, ПК-12); 4. Провести проектные расчеты элементов систем обеспечения информационной безопасности (ОПК-2, ОПК-3, ПК-8, ПК-10); 5. Предложить меры по улучшению (совершенствованию) системы информационной безопасности предприятия (ОПК-7, ПК-5, ПК-6, ПК-12, ПК-14); 6. Обосновать технико-экономические расчеты по предложенным мерам совершенствования системы информационной безопасности предприятия (ПК-7, ПК-8). **Завершающий этап** Составить план практики, написать отчет (ОК-8).
Форма отчетности по практике	Отчет о прохождение практики

Аннотация
программы производственной (преддипломной) практики
Б2.П Производственная практика: преддипломная практика
направление подготовки
10.03.01 Информационная безопасность
образовательная программа
«Комплексная защита объектов информатизации»
Уровень образования
бакалавриат
Форма обучения
очная, очно-заочная

Цели и задачи практики	**Цель:** совершенствование качества профессиональной подготовки, приобретение практических навыков и компетенций; сбор материалов, необходимых для подготовки выпускной квалификационной работы. **Задачи:** - закрепление и расширение теоретических знаний студентов; - формирование компетенций в создании и применении информационных технологий и систем информационного обеспечения защиты информации; - совершенствование навыков решения информационных задач на конкретном рабочем месте; - закрепление практических навыков по направлению будущей профессии.
Способ и форма(ы) проведения практики	Производственная практика может проходить: в государственных, коммерческих и некоммерческих организациях; информационных подразделениях предприятий различных сфер деятельности, а так же научно-производственных организациях. Способы проведения производственной практики: стационарная; выездная. Форма проведения практики: дискретно.
Общая трудоемкость практики	В соответствии с учебным планом преддипломная практика проводится на 4 курсе, в 8 семестре для студентов очной формы обучения и на 5 курсе, 10 семестр для студентов очно-заочной формы обучения. Продолжительность практики составляет 8 недель. Общая трудоемкость преддипломной практики составляет 12 зачетных единиц, 432 часа.
Требования к результатам прохождения практики	
способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты	**Знать:** основы требования к профессиональной деятельности специалиста в области защиты информации; нормы профессиональной этики, взаимоотношения в коллективе; **Уметь:** работать с различными программно-аппаратными средствами защиты информации; соблюдать нормы профессиональной этики; **Владеть:** основными трудовыми функциями специалиста по защите информации, специфику работы на данном предприятии;

интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);	навыками профессионального общения.
способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);	**Знать:** основы взаимоотношений в коллективе; правила внутреннего распорядка организации; **Уметь:** выполнять возложенные функции специалиста по защите информации в коллективе; соблюдать правила и нормы охраны труда, техники безопасности, пожарной безопасности, правила внутреннего распорядка организации; **Владеть:** методами работы на конкретном рабочем месте; навыками проведения совместных работ и экспериментов в коллективе.
способностью к самоорганизации и самообразованию (ОК-8);	**Знать:** все задания, предусмотренные программой практики, и сроки их выполнения; методы и средства, необходимые для самостоятельного выполнения заданий практики; состав отчетных документов и способы их подготовки; самостоятельно выбрать применяемые ИТ инструменты. **Уметь:** самостоятельно составить индивидуальный план своей деятельности на практике; подготовить письменный отчет о прохождении практики и представить его в Институт для защиты в установленные сроки. **Владеть:** навыками самостоятельного сбора необходимой информации для разработки проекта по совершенствованию защиты информации на предприятии; написания отчета по практике; навыками составления отчета о проведенных работах в рамках практики.
способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);	**Знать:** необходимый математический аппарат для построения дифференцируемой модели предприятия; **Уметь:** построить модель взаимодействия структурных компонентов предприятия; **Владеть:** навыками построения дифференцируемой модели предприятия.
способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);	**Знать:** архитектуру предприятия, его виды деятельности, ИТ-инфраструктуру предприятия информационной безопасности; методы и технологии обработки информации; **Уметь:** проводить анализ архитектуры предприятия, его видов деятельности, ИТ-инфраструктуры и информационной безопасности; применять информационные технологии для поиска и обработки информации; **Владеть:** методами анализа структуры и содержания информационных процессов на предприятии; навыками построения ИТ инфраструктуры предприятия.
способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);	**Знать:** нормативные правовые акты по вопросам информационной безопасности, в том числе выбранного предприятия; **Уметь:** использовать нормативные материалы и стандарты в обосновании предложений по совершенствованию информационной безопасности предприятия;

	Владеть: навыками разработки нормативных правовых актов по защите информации предприятия.
способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);	**Знать:** методы выявления угроз информационной безопасности; способы защиты от угроз информационной безопасности; **Уметь:** выявлять проблемы в организации информационной безопасности предприятия; применять средства и способы защиты информации; **Владеть:** методами выявления угроз информационной безопасности; навыками поиска инновационных способов защиты от угроз информационной безопасности.
способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);	**Знать:** программные и аппаратные средства защиты информации; **Уметь:** использовать необходимые программные и аппаратные средства для защиты информации на предприятии; **Владеть:** навыками настройки и эксплуатации программно-аппаратных средств защиты информации.
способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);	**Знать:** политику информационной безопасности предприятия; **Уметь:** комплексно решать вопросы информационной безопасности; **Владеть:** методами реализации политики информационной безопасности объектов защиты.
способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);	**Знать:** методы анализа исходных данных для разработки проекта совершенствования информационной безопасности предприятия; **Уметь:** провести технико-экономическое обоснование проекта по совершенствованию информационной безопасности предприятия; **Владеть:** методами составления технико-экономического обоснования проекта по совершенствованию информационной безопасности предприятия.
способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);	**Знать:** технологию подготовки технической документации по информационной безопасности предприятия; **Уметь:** оформить техническую документацию ; **Владеть:** составлением рабочей документации по информационной безопасности предприятия.
способностью осуществлять подбор, изучение и обобщение научно-	**Знать:** основные документы и научно-техническую литературу по защите информации; **Уметь:** делать обзор и составлять список используемой

технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);	научно-технической и нормативной литературы; **Владеть:** навыками подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов.
способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);	**Знать:** способы защиты от угроз информационной безопасности, стандарты безопасности в информационных системах; **Уметь:** проводить анализ информационной безопасности деятельности предприятия с учетом новейших нормативных материалов по вопросам информационной безопасности и в соответствии с требованиями стандартов; **Владеть:** методами анализа информационной безопасности объектов и систем в соответствии с требованиями стандартов.
способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);	**Знать:** методы проведения экспериментов по защите информации, подбору способов и средств защиты информации, определение достоверности проводимых экспериментов; **Уметь:** провести эксперимент по заданной тематике, в том числе по подбору способов и средств защиты информации на предприятии; **Владеть:** методами проведения эксперимента по подбору способов и средств защиты информации на предприятии, обработку, оценку погрешности и достоверности результатов.
способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);	**Знать:** комплекс мер по обеспечению информационной безопасности; методы и средства управления процессом защиты информации на предприятии; **Уметь:** применять программные и аппаратные средства для обеспечения комплексной защиты информации; **Владеть:** методами и средствами комплексной защиты информации.
способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** программные средства для решения практических задач; документы ФСТЭК по защите информации ограниченного доступа; **Уметь:** организовывать технологический процесс защиты информации ограниченного доступа в соответствии с требованиями стандартов, в том числе решений ФСТЭК; **Владеть:** навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и документами ФСТЭК.

(ПК-15).	
Содержание практики	Требуемые компетенции формируются при выполнении следующих заданий по производственной практике. **Подготовительный этап** Формулирование конкретных задач практической деятельности студентов, доведение формы и содержания отчетной документации (ОК-5, ОК-8, ОПК-4); **Основной этап** 1. Провести анализ архитектуры предприятия, его видов деятельности, ИТ-инфраструктуры и информационной безопасности (ОК-6, ОПК-2, ОПК-4, ОПК-5, ОПК-7, ПК-2, ПК-10); 2. Выявить проблемы в организации информационной безопасности предприятия, в нерациональном использовании формальных и не формальных средств ИБ и т.п. (ОК-8, ОПК-4, ОПК-7) 3. Провести анализ угроз информационной безопасности для деятельности выбранного предприятия, найти способы защиты от них. Проконсультировать руководство и работников предприятия по вопросу их внедрения (ОК-6, ОК-8, ОПК-7, ПК-10, ПК-13); 4. Разработать и оформить проект по совершенствованию информационной безопасности предприятия (ОК-8, ПК-2, ПК-4, ПК-7, ПК-8, ПК-11, ПК-13, ПК-15); 5. Проконсультировать руководство и работников предприятия по вопросам совершенствования информационной безопасности, рационального выбора формальных и не формальных средств ИБ, применяемых на предприятии (ОК-5, ОК-6, ПК-9, ПК-10, ПК-13). **Завершающий этап** Предоставить отчетные документы по итогам прохождение практики (ОК-5, ОК-6, ОК-8, ПК-9). а) характеристику с места практики с подписью и печатью; б) отчет о прохождении практики; в) дневник практики. Отчет о практике должен содержать сведения о выполненных студентом работах в период практики, результаты исследований с последующими выводами
Форма отчетности по практике	Отчет о прохождение практики