

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 18.01.2025 13:02:58
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

АННОТАЦИИ ПРОГРАММ ПРАКТИК

Направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Образовательная программа (профиль):

«Безопасность открытых информационных систем»

Год начала обучения:

2024

Уровень образования:

Специалитет

Квалификация (степень) выпускника:

Специалист по защите информации

Форма обучения:

очная

Ознакомительная практика

1 Цели, задачи и планируемые результаты прохождения практики

К **основным целям** ознакомительной практики следует отнести:

- закрепление, расширение углубление и систематизацию знаний, полученных при изучении дисциплин профессионального цикла, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.

К **основным задачам** освоения ознакомительной практики следует отнести:

- изучение проблемы документооборота и терминологию в учреждениях, организациях и предприятиях разнообразных форм собственности и профиля;
- освоение электронного документооборота на предприятии.

В результате освоения производственной практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК—1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Знает основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных; ИОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; <ul style="list-style-type: none">• ИОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).
ПК-15. Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	ИПК-15.1. Знает: <ul style="list-style-type: none">• основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры. ИПК-15.2. Умеет: <ul style="list-style-type: none">• определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем. ИПК-15.3. Владеет методами формирования комплекса мер по защите информации и ограниченного доступа

2 Место практики в структуре образовательной программы

Учебная практика относится к базовой части блока Б2.1 «Практики» основной образовательной программы (Б2.1.1).

3 Характеристика практики

Тип и вид практики – учебная, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится на предприятиях различных форм собственности, кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 10 семестре на базе кафедры и на предприятиях различных форм собственности.

4 Структура и содержание практики

Общая трудоемкость практики составляет 3 зачетных единиц, 108 часов.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	
1	Современные проблемы документооборота и терминологию в учреждениях, организациях и предприятиях различных форм собственности и профиля.	Типовой состав документов предприятия – базы практики. Проблемы документирования информации. Формирование системы документации, обеспечивающей деятельность предприятия – базы практики. Унифицированная система документации предприятия – базы практики. Структура документа, нормативные требования к составлению и оформлению управленческих документов. Особенности языка служебных документов. Способы и средства документирования. Организация работы с документами. Реквизиты, обеспечивающие юридическую силу документа.	1	36	Домашние задания. Тесты. Раздел отчета.
2	Электронный документооборот на предприятии.	Программное обеспечение документирования. Средства защиты электронных документов. Управление электронными документами. Управление деловыми процессами. Канцелярия. Управление совещаниями и заседаниями. Управление взаимодействием с клиентами. Управление договорами. Обращения граждан и организаций. Интеграция с системами обмена документами.	2	72	Раздел отчета.

Проектно-технологическая практика

1 Цели, задачи и планируемые результаты прохождения практики

К **основным целям** освоения проектно-технологической практики следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации при реализации и внедрении системы информационной безопасности на предприятии;
- приобретение и развитие необходимых практических умений и навыков при реализации и внедрении системы информационной безопасности на предприятии в соответствии с требованиями к уровню подготовки выпускника.

К **основным задачам** освоения проектно-технологической практики следует отнести:

- получение практических навыков при реализации и внедрении средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- получение практических навыков эксплуатации средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- овладение методов и средств, связанных с реализацией частных политик информационной безопасности автоматизированной системы,
- осуществление мониторинга и аудита безопасности автоматизированной системы на предприятии.

В результате освоения производственной практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ИОПК-4.1 Знает: <ul style="list-style-type: none">• Основные законы механики;• Основные законы термодинамики и молекулярной физики;• Основные законы электричества и магнетизма;• Основы квантовой физики и физики твердого тела;• Основы теории колебаний и волн, оптики;• Физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации. ИОПК-4.2 Умеет:

	<ul style="list-style-type: none"> • строить математические модели физических явлений и процессов; • решать типовые прикладные физические задачи; • анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; • применять математические методы исследования моделей шифров; • основы физической защиты объектов информатизации. <p>ИОПК-4.3 Владеет:</p> <ul style="list-style-type: none"> • методами теоретического исследования физических явлений и процессов; • навыками проведения физического эксперимента и обработки его результатов.
<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации</p>	<p>ИОПК-5.1. Знает основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;</p> <p>ИОПК-5.2. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, пользоваться нормативными документами по защите информации;</p> <p>ИОПК-5.3. Владеет навыками работы с нормативными правовыми актами.</p>
<p>ПК-12. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p>	<p>ИПК-12.1. Знает:</p> <ul style="list-style-type: none"> • состав системы управления и требования к ее элементам; • основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. <p>ИПК-12.2. Умеет:</p> <ul style="list-style-type: none"> • эффективно использовать различные методы и средства защиты информации для компьютерных сетей; <p>ИПК-12.3. Владеет методами проведения выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</p>
<p>ОПК—11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем</p>	<p>ИОПК-11.1. Знает программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях.</p> <p>ИОПК-11.2. Умеет проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</p> <p>ИОПК-11.3. Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками работы с нормативными правовыми актами; навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита)</p>

	баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.
ПК-16. Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	<p>ИПК-16.1. Знает:</p> <ul style="list-style-type: none"> • основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; • -основные методы управления информационной безопасностью. <p>ИПК-16.2. Умеет:</p> <ul style="list-style-type: none"> • восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; • разрабатывать частные политики информационной безопасности автоматизированных систем. <p>ИПК-16.3. Владеет:</p> <ul style="list-style-type: none"> • навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; • навыками организации и обеспечения режима секретности; • навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; • навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; • навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.
ПК-17. Способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	<p>ИПК-17.1. Знает:</p> <ul style="list-style-type: none"> • основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; • основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации. <p>ИПК-17.2. Умеет:</p> <ul style="list-style-type: none"> • использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; • оценивать эффективность и надежность защиты операционных систем; • планировать политику безопасности операционных систем • эффективно использовать различные методы и средства защиты информации для компьютерных сетей; • применять средства обеспечения безопасности

	<p>данных;</p> <ul style="list-style-type: none"> • проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. <p>ИПК-17.3. Владеет:</p> <ul style="list-style-type: none"> • навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; • навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; • методами формирования требований по защите информации; • методами управления информационной безопасностью автоматизированных систем; • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
<p>ПК-18. Способность администрировать подсистему информационной безопасности автоматизированной системы</p>	<p>ИПК-18.1. Знает:</p> <ul style="list-style-type: none"> • типовые шифры с открытыми ключами; • технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; • источники и классификацию угроз информационной безопасности; • программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; • основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; • содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; • основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); • основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; • современные технологии и методы программирования. <p>ИПК-18.2. Умеет:</p> <ul style="list-style-type: none"> • планировать политику безопасности операционных систем; • применять средства обеспечения безопасности данных; • классифицировать и оценивать угрозы информационной безопасности для объекта

	<p>информатизации;</p> <ul style="list-style-type: none"> • администрировать подсистемы информационной безопасности автоматизированных систем. <p>ИПК-18.3. Владеет:</p> <ul style="list-style-type: none"> • навыками работы с операционными системами семейства Windows и Unix, восстановления операционных систем после сбоев; • навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; • навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; • навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; • навыками работы с технической документацией на ЭВМ и вычислительные системы; • профессиональной терминологией в области информационной безопасности; • навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; • навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы; • навыками разработки программной документации.
<p>ПК-19. Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы</p>	<p>ИПК-19.1. Знает типовые шифры с открытыми ключами.</p> <p>ИПК-19.2. Умеет реализовывать политику безопасности баз данных.</p> <p>ИПК-19.3. Владеет навыками использования типовых криптографических алгоритмов и навыками использования ЭВМ в анализе простейших шифров.</p>
<p>ПК-20. Способность управлять информационной безопасностью автоматизированной системы</p>	<p>ИПК-20.1. Знает основные методы управления информационной безопасностью.</p> <p>ИПК-20.2. Умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.</p> <p>ИПК-20.3. Владеет методами управления информационной безопасностью автоматизированных систем.</p>

2 Место практики в структуре образовательной программы

Проектно-технологическая практика относится к обязательной части блока Б2.2 «Практики» основной образовательной программы (Б2.2.1).

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3 Характеристика практики

Тип и вид практики – производственная, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 10 семестре на базе предприятий требуемого профиля.

4 Структура и содержание практики

Общая трудоемкость практики составляет 15 зачетных единиц, 540 часов.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	
1	Установка и настройка средств защиты информации в автоматизированной системе	Эксплуатационная документация на систему защиты информации автоматизированной системы, руководство администратора и пользователя средств защиты информации.	1	36	Раздел отчета. Установка и настройка средств защиты информации.
2	Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	Перечень лиц, имеющих доступ к объектам защиты информационной системы, и их права (привилегии) доступа к этим объектам, а также перечень лиц, имеющих доступ в помещения, в которых расположены технические средства обработки информации. Состав организационных мер и порядок их реализации. Порядок учета, хранения и использования съемных машинных носителей информации. Порядок вывода информации на внешние носители информации. Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей. Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты. Порядок обслуживания системы защиты информации обслуживающим персоналом.	1	36	Раздел отчета. Документы, определяющие мероприятия, проводимые оператором.
3	Внедрение организационных мер в информационной системе.	Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа	1	36	Раздел отчета. Документы по

		<p>субъектов доступа к объектам доступа (далее - правила разграничения доступа), и введение ограничений на действия пользователей и обслуживающего персонала, а так же на изменение условий эксплуатации, состава и конфигурации технических средств обработки информации и программного обеспечения. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.</p> <p>Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.</p>			организационным мерам.
4	Предварительные испытания системы защиты информации информационной системы	Проверка работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.	1	36	Раздел отчета. Предварительные испытания системы защиты информации информационной системы.
5	Опытная эксплуатация системы защиты информации информационной системы.	Проверка функционирования системы защиты информации информационной системы, в том числе реализованных мер по защите информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.	1	36	Раздел отчета. Опытная эксплуатация системы защиты информации информационной системы.
6	Анализ уязвимостей информационной системы	<p>Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.</p> <p>Средства контроля (анализа) защищенности информации.</p> <p>Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.</p> <p>Правильность установки и настройки средств защиты информации, технических средств обработки информации и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами обработки информации и программным обеспечением.</p> <p>Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.</p>	2	72	Раздел отчета. Анализ уязвимостей информационной системы.
7	Приемочные	Проверка выполнения требований к	1	36	Раздел

	испытания системы защиты информации информационной системы	системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.			отчета. Приемочные испытания системы защиты информации информационной системы.
8	Обеспечение безопасности среды эксплуатации информационной системы	<p>Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера, и средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.</p> <p>Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.</p> <p>Защита технических средств, средств защиты информации и средств обеспечения функционирования.</p>	2	72	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
9	Администрирование системы защиты информации информационной системы.	<p>Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.</p> <p>Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.</p> <p>Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).</p> <p>Внесение изменений в организационно-распорядительные документы по защите информации (при необходимости).</p> <p>Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.</p>	1	36	Раздел отчета. Администрирование системы защиты информации информационной системы.
10	Реагирование на инциденты, связанные с нарушением требований о защите информации.	<p>Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации, выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).</p> <p>Своевременное информирование структурного подразделения или должностного лица, ответственных за защиту информации, пользователями</p>	2	72	Раздел отчета. Реагирование на инциденты, связанные с нарушением требований о защите информации

		<p>информационной системы об инцидентах, связанных с нарушением требований о защите информации.</p> <p>Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации, планирование и принятие мер по предупреждению и устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов после сбоев, выявлению и устранению последствий внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).</p>			
11	Управление конфигурацией системы защиты информации автоматизированной системы	<p>Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.</p> <p>Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.</p> <p>Управление параметрами настройки средств защиты информации, составом и конфигурацией технических средств и программного обеспечения, а также контроль за несанкционированными подключениями технических средств и установкой программного обеспечения</p>	1	36	Раздел отчета. Управление конфигурацией системы защиты информации автоматизированной системы
12	Управление защитой информации в информационной системе	<p>Выполнение организационных мер по защите информации.</p> <p>Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.</p> <p>Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.</p> <p>Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.</p> <p>Периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер по защите информации в случае возникновения новых угроз безопасности информации.</p> <p>Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.</p>	1	36	Раздел отчета. Управление защитой информации в информационной системе

		<p>Доработка (модернизация) системы защиты информации информационной системы и ее переаттестация при изменении класса защищенности информационной системы, состава актуальных угроз безопасности информации или проектных решений по системе защиты информации информационной системы (в том числе состава используемых средств защиты информации).</p> <p>Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.</p>			
--	--	---	--	--	--

Научно-исследовательская работа

1 Цели, задачи и планируемые результаты прохождения практики

К **основным целям** освоения научно-исследовательской работы следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации при исследовании системы информационной безопасности на предприятии;
- приобретение и развитие необходимых практических умений и навыков при исследовании системы информационной безопасности на предприятии в соответствии с требованиями к уровню подготовки выпускника.

К **основным задачам** освоения научно-исследовательской работы следует отнести:

- получение практических навыков исследования средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- овладение методов и средств, связанных с реализацией частных политик информационной безопасности автоматизированной системы,
- осуществление мониторинга и аудита безопасности автоматизированной системы на предприятии.

В результате освоения производственной практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов с учетом оценки существующих рисков и возможностей их минимизации.
ПК-1 Способность создавать и исследовать модели автоматизированных систем.	ИПК-1.1. Знает: - модели шифров и математические методы их исследования; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации;

	<p>- требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования.</p> <p>ИПК-1.2. Умеет:</p> <ul style="list-style-type: none"> - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. <p>ИПК-1.3. Владеет:</p> <ul style="list-style-type: none"> - навыками математического моделирования в криптографии; - методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; - навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.
<p>ПК-2. Способность проводить анализ защищенности автоматизированных систем</p>	<p>ИПК-2.1. Знает:</p> <ul style="list-style-type: none"> - требования к шифрам и основные характеристики шифров; - модели шифров и математические методы их исследования; - программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; - технические каналы утечки информации; - возможности технических средств перехвата информации <p>ИПК-2.2. Умеет организовывать защиту информации от утечки по техническим каналам на объектах информатизации</p> <p>ИПК-2.3. Владеет:</p> <ul style="list-style-type: none"> - навыками организации и обеспечения режима секретности.
<p>ПК-3 Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p>	<p>ИПК-3.1. Знает:</p> <ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. <p>ИПК-3.2. Умеет:</p> <ul style="list-style-type: none"> - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - анализировать и оценивать угрозы информационной

	<p>безопасности объекта.</p> <p>ИПК-3.3. Владеет навыками организации и обеспечения режима защиты от угроз информационной безопасности объекта.</p>
<p>ПК-4. Способность проводить анализ рисков информационной безопасности автоматизированной системы</p>	<p>ИПК-4.1. Знает:</p> <ul style="list-style-type: none"> - требования к шифрам и основные характеристики шифров. <p>ИПК-4.2. Умеет:</p> <ul style="list-style-type: none"> - анализировать и оценивать угрозы информационной безопасности объекта. <p>ИПК-4.3. Владеет методами проведения анализа рисков информационной безопасности объекта</p>
<p>ПК-5. Способность проводить анализ, предлагать и обосновывать выбор решений обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p>	<p>ИПК-5.1. Знает:</p> <ul style="list-style-type: none"> - требования к шифрам и основные характеристики шифров; - архитектуру, принципы функционирования, электронную базу современных компьютеров, вычислительных и телекоммуникационных систем; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основные информационные технологии, используемые в автоматизированных системах; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. <p>ИПК-5.2. Умеет:</p> <ul style="list-style-type: none"> - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. <p>ИПК-5.3. Владеет:</p> <ul style="list-style-type: none"> - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - методами формирования требований по защите информации; - методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; - профессиональной терминологией в области информационной безопасности; - навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.
<p>ОПК—8. Способен применять методы научных исследований при проведении разработок в области защиты информации в</p>	<p>ИОПК-8.1. Знает методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;</p>

автоматизированных системах	ИОПК-8.2. Умеет применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах ОПК-8.3 Владеет методами научных исследований при проведении разработок в области защиты информации в автоматизированных системах.
-----------------------------	---

2 Место практики в структуре образовательной программы

Научно-исследовательская работа относится к обязательной части блока Б2.2 «Практики» основной образовательной программы (Б2.2.2).

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3 Характеристика практики

Тип и вид практики –научно-исследовательская, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 11 семестре на базе предприятий требуемого профиля.

4 Структура и содержание практики

Общая трудоемкость практики составляет 12 зачетных единицы, 432 часов.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	
1	Модели автоматизированной системы.	Функциональная модель IDEF0 информационной системы. AS-IS. Функциональная модель IDEF0 информационной системы. TO-BE. Диаграммы поведения Use Case безопасной информационной системы. Диаграммы поведения Statechart безопасной информационной системы. Диаграммы поведения Activity безопасной информационной системы. Диаграммы поведения Collaboration & Sequence.	2	72	Раздел отчета.
2	Анализ защищенности автоматизированной системы.	Классификация информационной системы.	2	72	Раздел отчета.
3	Модели угроз и модели нарушителя информационной	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.	2	72	Раздел отчета.

	безопасности автоматизированной системы.				
4	Анализ рисков информационной безопасности автоматизированной системы.	Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Расчет информационных рисков.	2	72	Раздел отчета.
5	Разработка мероприятий по снижению информационных рисков.	Определение IT – технологий, требующих снижения информационного риска. Внедрение мер защиты в информационной системе для снижения рисков. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы.	4	144	Раздел отчета.

Преддипломная практика

1 Цели, задачи и планируемые результаты прохождения практики

К **основным задачам** освоения преддипломной практики следует отнести:

- ознакомление с должностными обязанностями сотрудников организации по профилю подготовки;
- освоение способов комплексного применения средств обеспечения информационной безопасности объекта защиты и оценки эффективности принимаемых мер.

К **основным целям** освоения преддипломной практики следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации;
- приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника.

В результате освоения производственной практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-8. Способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	ИПК-8.1. Знает: <ul style="list-style-type: none">• требования к шифрам и основные характеристики шифров;• основные информационные технологии, используемые в автоматизированных системах. ИПК-8.2. Умеет: <ul style="list-style-type: none">• контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем. ИПК-8.3. Владеет: <ul style="list-style-type: none">• навыками участия в экспертизе состояния защищенности информации на объекте защиты;• навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;• - методами расчета и• инструментального контроля показателей технической защиты информации;• навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;• методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;• методами оценки информационных рисков.
ПК-9. Способность участвовать в проведении экспериментально-исследовательских работ при	ИПК-9.1. Знает: <ul style="list-style-type: none">• требования к шифрам и основные

<p>сертификации средств защиты информации автоматизированных систем</p>	<p>характеристики шифров;</p> <ul style="list-style-type: none"> • способы и средства защиты информации от утечки по техническим каналам и контроля эффективности • защиты информации. <p>ИПК-9.2. Умеет проводит экспериментально-исследовательские работы при сертификации средств защиты информации автоматизированных систем,</p> <p>ИПК-9.3. Владеет навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем.</p>
<p>ПК-10. Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации</p>	<p>ИПК-10.1. Знает:</p> <ul style="list-style-type: none"> • возможности технических средств перехвата информации. <p>ИПК-10.2. Умеет проводить экспериментально-исследовательские работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации.</p> <p>ИПК-10.3 Владеет навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.</p>
<p>ОПК—13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем</p>	<p>ИОПК-13.1. Знает методы и средства диагностики и тестирования систем защиты информации автоматизированных систем;</p> <p>ИОПК-13.2. Умеет проводить анализ уязвимостей систем защиты информации автоматизированных систем.</p> <p>ИОПК-13.3. Владеет способами организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем и проведением анализа уязвимости.</p>
<p>ПК-11. Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p>	<p>ИПК-11.1. Знает:</p> <ul style="list-style-type: none"> • основные понятия и методы в области управленческой деятельности; • порядок выработки и реализации управленческих решений; • содержание управленческой работы руководителя подразделения; • проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; • содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. <p>ИПК-11.2. Умеет:</p> <ul style="list-style-type: none"> • оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; • осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; • проводить мониторинг угроз безопасности компьютерных сетей; • контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; • администрировать подсистемы

	<p>информационной безопасности автоматизированных систем.</p> <p>ИПК-11.3. Владеет:</p> <ul style="list-style-type: none"> • навыками обоснования, выбора, реализации и контроля результатов управленческого решения; • навыками организации и обеспечения режима секретности; • навыками работы с технической документацией на ЭВМ и вычислительные системы.
<p>ПК-12. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p>	<p>ИПК-12.1. Знает:</p> <ul style="list-style-type: none"> • - состав системы управления и требования к ее элементам; • - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. <p>ИПК-12.2. Умеет:</p> <ul style="list-style-type: none"> • - эффективно использовать различные методы и средства защиты информации для компьютерных сетей; <p>ИПК-12.3. Владеет методами проведения выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</p>
<p>ОПК—14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений</p>	<p>ИОПК-14.1. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.</p> <p>ИОПК-14.2. Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности автоматизированных систем.</p> <p>ИОПК-14.3. Владеет методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации.</p>
<p>ПК-13. Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p>	<p>ИПК-13.1. Знает ГОСТы по оформлению документов по разработке и регламентированию по обеспечению информационной безопасности.</p> <p>ИПК-13.2. Умеет:</p>

	<ul style="list-style-type: none"> • разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; • разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. <p>ИПК-13.3. Владеет:</p> <ul style="list-style-type: none"> • навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, • программных систем с учетом требований по обеспечению информационной безопасности.
<p>ПК-14. Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p>	<p>ИПК-14.1. Знает:</p> <ul style="list-style-type: none"> • основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. <p>ИПК-14.2. Умеет:</p> <ul style="list-style-type: none"> • эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; • контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; • разрабатывать частные политики информационной безопасности автоматизированных систем. <p>ИПК-14.3. Владеет:</p> <ul style="list-style-type: none"> • криптографической терминологией; • навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
<p>ПК-15. Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p>	<p>ИПК-15.1. Знает:</p> <ul style="list-style-type: none"> • основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры. <p>ИПК-15.2. Умеет:</p> <ul style="list-style-type: none"> • определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем. <p>ИПК-15.3. Владеет методами формирования комплекса мер по защите информации и ограниченного доступа.</p>

2 Место практики в структуре образовательной программы

Преддипломная практика относится к базовой части блока Б2.2 «Практики» основной образовательной программы (Б2.2.3).

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3 Характеристика практики

Тип и вид практики – преддипломная, стационарная.

Способ и форма проведения практики – непрерывно.

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 11 семестре на базе предприятий требуемого профиля.

4 Структура и содержание практики

Общая трудоемкость практики составляет 12 зачетных единиц, 432 часа.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	
1	Структура, история и традиции организации	Структура, история и традиции организации. Нормативные документы, регламентирующие деятельность организации. Основные обязанности должностных лиц организации по профилю подготовки.	1	36	Раздел отчета
2	Основные технологические процессы	Основные технологические процессы и производственное оборудование по профилю деятельности.	2	72	Раздел отчета
3	Стандарты и условия	Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.	2	72	Раздел отчета
4	Технологии защиты информации на предприятии	Функциональные обязанности сотрудника организации по должности, определенной на период практики. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.	4	144	Раздел отчета
5	Методики защиты	Методики применения	3	108	Раздел отчета

	информации	измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.			
--	------------	--	--	--	--