АННОТАЦИИ РАБОЧИХ ПРОГРАММ ПРАКТИК

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника

Специалист

Форма обучения

Очная

Год приема – 2019

УЧЕБНАЯ ПРАКТИКИ

1. Цели практики

К **основным целям** учебной 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.

2. Задачи практики

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

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

3. Место практики в структуре программы

Учебная практика относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

4. Тип, вид, способ и формы проведения практики

Тип и вид практики – учебная, стационарная.
Способ и форма проведения практики – непрерывно.

5. Место и время проведения практики

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

Практика проводится в 6 семестре на базе кафедры и на предприятиях различных форм собственности (2 недели).

6. Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения практики по получению первичных профессиональных умений у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по практике**

ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;	**знать:** - социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства; **уметь:** -соблюдать нормы профессиональной этики;
ОПК-4	способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах;	**знать:** - значение информации в развитии современного общества; **уметь:** -определять информационные ресурсы, подлежащие защите; -применять информационные технологии для поиска и обработки информации; **владеть:** - методами и средствами электронного документооборота;
ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;	**уметь:** - формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

7. 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 документоведения и терминологию в учреждениях, организациях и предприятиях разнообразных 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	1	36	Домащние задания. Тесты. Раздел отчета.

		требования к составлению и оформлению управленческих документов. Особенности языка служебных документов. Способы и средства документирования. Организация работы с документами. Реквизиты, обеспечивающие юридическую силу документа.			
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.

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

1. Цели практики

К **основным целям** освоения производственной 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.

2. Задачи практики

К **основным задачам** освоения производственной 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.

3. Место практики в структуре программы

Производственная практика относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

4. Тип, вид, способ и формы проведения практики

Тип и вид практики – производственная, стационарная.

Способ и форма проведения практики – непрерывно.

5. Место и время проведения практики

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 недели).

6. Компетенции обучающегося, формируемые в результате прохождения практики

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

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по практике**
ПК-10	способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных	**уметь:** - применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;

	компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;	
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы;	**знать:** -состав и структуру политики информационной безопасности автоматизированной системы предприятия; **уметь:** - разрабатывать политику информационной безопасности автоматизированной системы;
ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;	**уметь:** - участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы ;	**уметь:** - участвовать в проектировании средств защиты информации автоматизированной системы; **владеть:** -методами и средствами проектирования средств защиты.
ПК-24	способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;	**знать:** IT –технологии, применяемые на предприятии и защищаемые информационные ресурсы; **уметь:** использовать IT –технологии, применяемые на предприятии, с учетом требований информационной безопасности;
ПК-25	способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;	**знать:** средства защиты информационно-технологических ресурсов автоматизированной системы на предприятии; **уметь:** эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы; **владеть:**

		методами и средствами восстановления их работоспособности при возникновении нештатных ситуаций;
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы;	**уметь:** администрировать подсистему информационной безопасности автоматизированной системы;
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы ;	**знать:** политику информационной безопасности автоматизированной системы предприятия; **уметь:** выполнять работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы на предприятии; **владеть:** методами, связанные с реализацией частных политик информационной безопасности автоматизированной системы, мониторинга и аудита безопасности автоматизированной системы на предприятии;
ПК-28	способностью управлять информационной безопасностью автоматизированной системы.	**знать:** методы управления информационной безопасностью автоматизированной системы; **уметь:** управлять информационной безопасностью автоматизированной системы на предприятии.

7. Структура и содержание практики

Общая трудоемкость практики составляет 6 зачетных единицы, 216 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	Эксплуатационная документация на систему защиты	0,5	18	Раздел отчета.

	защиты информации в автоматизированной системе	информации автоматизированной системы, руководство администратора и пользователя средств защиты информации.			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.	0,5	18	Раздел отчета. Документы, определяющих мероприятия, проводимые оператором.
3	Внедрение организационных мер в информационной системе.	Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа), и введение ограничений на действия пользователей и обслуживающего персонала, а так же на изменение	0,5	18	Раздел отчета. Документы по организационным мерам.

		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. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.			
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.	0,5	18	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.	0,3	12	Раздел отчета. Опытная эксплуатация системы защиты информации информационной системы.
6	Анализ уязвимостей информационной системы	Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации. Средства контроля (анализа)	0,3	12	Раздел отчета. Анализ уязвимостей информационной

		защищенности информации. Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы. 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. Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.			системы.
7	Приемочные испытания системы защиты информации информационной системы	Проверка выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.	0,3	12	Раздел отчета. Приемочные испытания системы защиты информации информационной системы.
8	Обеспечение безопасности среды эксплуатации информационной системы	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.	1	36	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения

		Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены. Защита технических средств, средств защиты информации и средств обеспечения функционирования.			функционирования.
9	Администрирование системы защиты информации информационной системы.	Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности). Внесение изменений в организационно-распорядительные документы по защите информации (при необходимости). Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.	0,5	18	Раздел отчета. Администрирование системы защиты информации информационной системы.
10	Реагирование на инциденты, связанные с нарушением требований о защите информации.	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	0,5	18	Раздел отчета. Реагирование на инциденты, связанные с нарушением

		пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности). Своевременное информирование структурного подразделения или должностного лица, ответственных за защиту информации, пользователями информационной системы об инцидентах, связанных с нарушением требований о защите информации. 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).			требований о защите информации
11	Управление конфигурацией системы защиты информации автоматизированной системы	Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками. Управление параметрами настройки средств защиты информации, составом и конфигурацией технических средств и программного обеспечения, а также	0,5	18	Раздел отчета. Управление конфигурацией системы защиты информации автоматизированной системы

		контроль за несанкционированными подключениями технических средств и установкой программного обеспечения			
12	Управление защитой информации в информационной системе	Выполнение организационных мер по защите информации. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности. 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. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе. Доработка (модернизация) системы защиты информации информационной системы и ее переаттестация при изменении класса защищенности информационной системы, состава актуальных угроз безопасности	0,5	18	Раздел отчета. Управление защитой информации в информационной системе

		информации или проектных решений по системе защиты информации информационной системы (в том числе состава используемых средств защиты информации). Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.			

Научно-исследовательская работа

8. Цели 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.

9. Задачи практики

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.

10. Место практики в структуре программы

Научно-исследовательская работа относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

11. Тип, вид, способ и формы проведения практики

Тип и вид практики –научно-исследовательская, стационарная.

Способ и форма проведения практики – непрерывно.

12. Место и время проведения практики

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 недели).

13. Компетенции обучающегося, формируемые в результате прохождения практики

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

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по практике**
ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;	**уметь:** - осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
ПК-2	способностью создавать и исследовать модели автоматизированных систем;	**знать:** - модели автоматизированных систем; **уметь:** -проводить анализ защищенности автоматизированных систем **владеть:** -методами создания моделей автоматизированных систем;
ПК-3	способностью проводить анализ защищенности автоматизированных систем;	**уметь:** - проводить анализ защищенности автоматизированных систем;

		владеть: - инструментальными средствами анализа защищенности автоматизированных систем;
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;	**уметь:** - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы;	**уметь:** - проводить анализ рисков информационной безопасности автоматизированной системы; **владеть:** - методами анализа рисков информационной безопасности автоматизированной системы;
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;	**уметь:** - проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;	**уметь:** - разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

14. Структура и содержание практики

Общая трудоемкость практики составляет 6 зачетных единицы, 316 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	1	36	Раздел отчета.

		Case безопасной информационной системы. иаграммы поведения Statechart безопасной информационной системы. Диаграммы поведения Activity безопасной информационной системы. Диаграммы поведения. Collaboration & Sequence.			
2	Анализ защищенности автоматизированной системы.	Классификация информационной системы.	1	36	Раздел отчета.
3	Модели угроз и модели нарушителя информационной безопасности автоматизированной системы.	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.	1	36	Раздел отчета.
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.	1	36	Раздел отчета.
5	Разработка мероприятий по снижению информационных рисков.	Определение IT – технологий, требующих снижения информационного риска. Внедрение мер зашиты в информационной системе для снижения рисков. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы.	2	72	Раздел отчета.

ПРЕДДИПЛОМНАЯ ПРАКТИКА

15. Цели практики

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.

16. Задачи 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.

17. Место практики в структуре программы

Преддипломная практика относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

18. Тип, вид, способ и формы проведения практики

Тип и вид практики – преддипломная, стационарная.

Способ и форма проведения практики – непрерывно.

19. Место и время проведения практики

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 (8 недель).

20. Компетенции обучающегося, формируемые в результате прохождения практики

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

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по практике**

ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;	**уметь:** - проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; **владеть:** - методами и средствами контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-15	способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;	**знать:** - процедуру сертификации средств защиты информации; **уметь:** - проводить экспериментально-исследовательские работы при сертификации средств защиты информации;
ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;	**знать:** - процедуру аттестации автоматизированных систем с учетом нормативных документов по защите информации; **уметь:** - проводить экспериментально-исследовательские работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;	**уметь:** - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; **владеть:** - методами и инструментальными средствами мониторинга защищенности информации в автоматизированной системе;
ПК-18	способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;	**уметь:** - организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;

ПК-19	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;	**знать:** - систему управления информационной безопасностью автоматизированной системы; **уметь:** - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;	**уметь:** - организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;	**знать:** - состав, структуру и содержание документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; **уметь:** - разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
ПК-22	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;	**уметь:** - формировать политику информационной безопасности организации и контролировать эффективность ее реализации;
ПК-23	способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;	**уметь:** - формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	**уметь:** разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах

ПСК-7.2	Способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	**уметь:** проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах
ПСК-7.3	Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	**уметь:** проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем
ПСК-7.4	Способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	**уметь:** проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах
ПСК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	**уметь:** координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

21. 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	Действующие стандарты,	2	72	Раздел

	условия	технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.			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 информации	Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.	3	108	Раздел отчета