МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
проектно-технологической практики

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль подготовки)
«Безопасность открытых информационных систем»

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2022

Москва 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты прохождении 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: • 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 защиты информации. ИОПК-4.2 Умеет: • 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. ИОПК-4.3 Владеет: • методами теоретического исследования физических явлений и процессов; • навыками проведения физического эксперимента и обработки его результатов.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	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; ИОПК-5.2. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, пользоваться нормативными документами по защите информации; ИОПК-5.3. Владеет навыками работы с нормативными правовыми актами.
ПК-12. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	ИПК-12.1. Знает: • состав системы управления и требования к ее элементам; • основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. ИПК-12.2. Умеет: • эффективно использовать различные методы и средства защиты информации для компьютерных сетей; 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.
ОПК—11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИОПК-11.1. Знает программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах. системах управления базами данных, компьютерных сетях. 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. 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) 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	ИПК-16.1. Знает: • основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; • -основные методы управления информационной безопасностью. ИПК-16.2. Умеет: • восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; • разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК-16.3. Владеет: • 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	ИПК-17.1. Знает: • 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. ИПК-17.2. Умеет: • 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 данных; • проводить выбор программно-аппаратных

	средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. ИПК-17.3. Владеет: • 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.
ПК-18. Способность администрировать подсистему информационной безопасности автоматизированной системы	ИПК-18.1. Знает: • 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. ИПК-18.2. Умеет: • планировать политику безопасности операционных систем; • применять средства обеспечения безопасности данных; • классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; • администрировать подсистемы

	информационной безопасности автоматизированных систем. ИПК-18.3. Владеет: • 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.
ПК-19. Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	ИПК-19.1. Знает типовые шифры с открытыми ключами. ИПК-19.2. Умеет реализовывать политику безопасности баз данных. ИПК-19.3. Владеет навыками использования типовых криптографических алгоритмов и навыками использования ЭВМ в анализе простейших шифров.
ПК-20. Способность управлять информационной безопасностью автоматизированной системы	ИПК-20.1. Знает основные методы управления информационной безопасностью. ИПК-20.2. Умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. ИПК-20.3. Владеет методами управления информационной безопасностью автоматизированных систем.

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, 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	1	36	Раздел отчета. Документы по

		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. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.			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	Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации. Средства контроля (анализа) 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.	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	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. 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.	2	72	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения 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.	1	36	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 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	2	72	Раздел отчета. Реагирование на инциденты, связанные с нарушением требований о защите информации

		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).			
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 контроль за несанкционированными подключениями технических средств и установкой программного обеспечения	1	36	Раздел отчета. Управление конфигурацией системы защиты информации автоматизированной системы
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.	1	36	Раздел отчета. Управление защитой информации в информационной системе

		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). Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.				

5 Учебно-методическое и информационное обеспечение

5.1 Нормативные документы и ГОСТы

06.032 Специалист по безопасности компьютерных систем и сетей.

06.033 Специалист по защите информации в автоматизированных системах.

5.2 Основная литература

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

5.3 Дополнительная литература

Определяется предприятием.

5.4 Электронные образовательные ресурсы

Определяется предприятием.

5.5 Лицензионное и свободно распространяемое программное обеспечение

Определяется предприятием.

5.6 Современные профессиональные базы данных и информационные справочные системы

Определяется предприятием.

6 Материально-техническое обеспечение практики

Материально-техническое обеспечение практики определяется предприятием.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем».

7 Методические рекомендации

7.1 Методические рекомендации для руководителя по организации практики

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной практикой по получению профессиональных умений и профессионального опыта, осуществляется в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение практики на месте ее проведения руководителем практики от предприятия.

7.2 Методические указания для обучающихся по освоению дисциплины

Контрольные вопросы и задания для проведения аттестации по итогам практики

1. Эксплуатационная документация на систему защиты информации автоматизированной системы,
2. Руководство администратора и пользователя средств защиты информации.
3. Состав организационных мер и порядок их реализации.
4. Порядок учета, хранения и использования съемных машинных носителей информации.
5. Порядок вывода информации на внешние носители информации.
6. Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей.
7. Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты.
8. Порядок обслуживания системы защиты информации обслуживающим персоналом.
9. Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа).
10. 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.
11. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.
12. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.
13. Проверка работоспособности системы защиты информации информационной системы.
14. Принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.
15. Опытная эксплуатация системы защиты информации информационной системы
16. 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.
17. Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности

информации.

18. Средства контроля (анализа) защищенности информации.
19. Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.
20. 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.
21. Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.
22. Проверка выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.
23. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
24. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
25. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
26. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
27. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
28. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
29. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
30. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
31. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
32. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
33. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
34. 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).
35. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
36. Установка обновлений программного обеспечения, включая программное

обеспечение средств защиты информации, выпускаемых их разработчиками.

37. 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
38. Выполнение организационных мер по защите информации.
39. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
40. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
41. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
42. 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.
43. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
44. 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).
45. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.

8 Фонд оценочных средств

8.1 Методы контроля и оценивания результатов прохождения практики

В качестве основной формы отчетности является письменный отчет. Форма контроля прохождения практики - дифференцированный зачет.

8.2 Шкала и критерии оценивания результатов прохождения практики

По окончании практики студент-практикант составляет письменный отчет и в порядке, установленном кафедрой, сдает его и другие отчетные материалы, предусмотренные методическими указаниями кафедры к прохождению практики, подписанные руководителем практики от организации.

Отчет должен содержать сведения о конкретно выполненной студентом работе в период прохождения практики.

При оценке итогов работы студента принимается во внимание характеристика, данная ему руководителем практики от предприятия.

8.3 Оценочные средства

8.3.1 Текущий контроль

Отчет по практике.Отчет о практике должен содержать:

1. Установка и настройка средств защиты информации в автоматизированной системы.
2. Разработка документов, определяющих мероприятия, проводимые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации.
3. Внедрение организационных мер в информационной системе.
4. Предварительные испытания системы защиты информации информационной системы.
5. Опытная эксплуатация системы защиты информации информационной системы.
6. Анализ уязвимостей информационной системы.
7. Приемочные испытания системы защиты информации информационной системы
8. Обеспечение безопасности среды эксплуатации информационной системы
9. Администрирование системы защиты информации информационной системы.
10. Реагирование на инциденты, связанные с нарушением требований о защите информации.
11. Управление конфигурацией системы защиты информации автоматизированной системы
12. Управление защитой информации в информационной системе

8.3.2 Промежуточная аттестация

Дифференцированный зачет. Вопросы для дифференцированного зачета:

1. Эксплуатационная документация на систему защиты информации автоматизированной системы,
2. Руководство администратора и пользователя средств защиты информации.
3. Состав организационных мер и порядок их реализации.
4. Порядок учета, хранения и использования съемных машинных носителей информации.
5. Порядок вывода информации на внешние носители информации.
6. Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей.
7. Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты.
8. Порядок обслуживания системы защиты информации обслуживающим персоналом.
9. Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа).
10. 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.
11. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.
12. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.
13. Проверка работоспособности системы защиты информации информационной системы.
14. Принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.
15. Опытная эксплуатация системы защиты информации информационной системы

16. 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.
17. Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.
18. Средства контроля (анализа) защищенности информации.
19. Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.
20. 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.
21. Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.
22. Проверка выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.
23. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
24. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
25. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
26. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
27. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
28. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
29. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
30. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
31. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
32. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
33. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
34. 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).

35. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
36. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
37. 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
38. Выполнение организационных мер по защите информации.
39. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
40. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
41. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
42. 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.
43. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
44. 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).
45. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.