МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА
производственной практики

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль подготовки)

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация выпускника

Специалист

Форма обучения

Очная

Год приема - 2019

Москва 2019 г.

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 компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;	**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;
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 защиты информации в автоматизированной системе	Эксплуатационная документация на систему защиты информации автоматизированной системы, руководство администратора и пользователя средств защиты информации.	0,5	18	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.	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	0,5	18	Раздел отчета. Документы по организаци

		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.			онным 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.	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) защищенности информации.	0,3	12	Раздел отчета. Анализ уязвимостей информационной системы.

		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.			
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. 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	1	36	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения функционирования.

		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.	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 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	0,5	18	Раздел отчета. Реагирование на инциденты, связанные с нарушением требований о защите информации

		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	0,5	18	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	0,5	18	Раздел отчета. Управление защитой информации в информационной системе

		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 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.				

8. Научно-исследовательские и научно-производственные технологии, используемые на практике

Научно-исследовательские и научно-производственные технологии, используемые на практике, определяются предприятием.

9. Учебно-методическое обеспечение самостоятельной работы студентов на практике

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.

10. Формы промежуточной аттестации (по итогам практики)

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

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.

11. Учебно-методическое и информационное обеспечение практики

а) основная литература:

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

б) дополнительная литература:

определяется предприятием

в) программное обеспечение и интернет-ресурсы:

определяется предприятием

12. 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».

Программу составил: доцент, к.т.н Федоров Н.В.

Программа утверждена на заседании кафедры «Информационная безопасность» «29» августа 2019 г., протокол № 1.

Заведующий кафедрой

профессор, к. т. н. Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский политехнический университет

Направление подготовки:
10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль):
«Обеспечение информационной безопасности распределенных информационных систем»
Виды профессиональной деятельности: научно-исследовательская, проектно-конструкторская, контрольно-аналитическая, организационно-управленческая, эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Состав: 1. Паспорт фонда оценочных средств
2. Оценочные средства для текущей аттестации
3. Оценочные средства для промежуточной аттестации

Составитель:

доцент, к.т.н. Федоров Н.В.

Москва, 2019 год

1. Паспорт фонда оценочных средств

Таблица 1

Производственная практика					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК-10	способностью 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;	**уметь:** - применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов ащищенных автоматизированных истем в сфере профессиональной деятельности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -- применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных омпонентов 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;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: Знать состав и структуру политики информационной безопасности автоматизированной системы предприятия; Повышенный уровень: азрабатывать 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;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - 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	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - участвовать в проектировании средств защиты информации автоматизированной системы; Повышенный уровень: 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;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -- использовать IT –технологии, применяемые на предприятии, с учетом требований информационной безопасности; Повышенный уровень: - внедрять новые IT –технологии 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:** редства защиты информационно-технологических ресурсов автоматизированной системы на предприятии; **уметь:** эффективно применять средства защиты информационно-технологических ресурсов автоматизированной системы; **владеть:** методами и средствами восстановления их	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -применять средства защиты информационно-технологических ресурсов автоматизированной системы, используемые на предприятии; Повышенный уровень: - внедрять новые средства защиты информационно-технологических ресурсов автоматизированной системы;
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы;	**уметь:** администрировать подсистему информационной безопасности автоматизированной системы;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - администрировать подсистему информационной безопасности автоматизированной системы; Повышенный уровень: - администрировать систему 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:**	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: выполнять работы, связанные с реализацией частных политик информационной безопасности автоматизированной системы; Повышенный уровень: осуществлять мониторинг и аудит 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.	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -управлять подсистемой информационной безопасности автоматизированной системы на предприятии. Повышенный уровень: - управлять информационной безопасностью автоматизированной системы на предприятии.

2. Оценочные средства для текущей аттестации

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

3. Оценочные средства для промежуточной аттестации

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.