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

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
производственной практики

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2020

Москва 2020 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 для формирования требований и разработке системы защиты информации автоматизированной системы;
- приобретение и развитие необходимых практических умений и навыков при формировании требований и разработке 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 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 блоку 2 «Практики» основной образовательной программы.

Практика базируется на дисциплинах базовой и вариативной части учебного плана.

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 8 семестре на базе предприятий требуемого профиля.

6. Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения проектно-технологической 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 выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	**уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;	**знать:** программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; **уметь:** применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты;	**уметь:** администрировать подсистемы информационной безопасности объекта защиты;
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;	**знать:** политики информационной безопасности; **уметь:** проводить реализацию политики информационной безопасности, **владеть:** комплексным подходом к обеспечению информационной безопасности объекта защиты;
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	**уметь:** принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	**уметь:** принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	**знать:** техническую документацию с учетом действующих нормативных и методических документов; **уметь:** оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

7. Структура и содержание практики

Общая трудоемкость практики составляет 9 зачетных единиц, 324 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	Определение актуальных угроз безопасности информации и разработку на их основе модели угроз	Оценка возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей информационной системы, возможных последствий от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности), а также с учетом структурно-функциональных характеристик информационной системы, включающих структуру и состав информационной системы, физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами, режимы обработки информации в информационной системе в целом и в ее отдельных сегментах. Модель угроз безопасности информации.	1	36	Модель угроз
2	Классификация информационной системы	Определение значимости обрабатываемой информации конфиденциального характера и масштаба информационной системы. Класс защищенности.	1	36	Класс защищенности
3	Определение требований к системе защиты информации информационной системы	Цель и задачи обеспечения защиты информации в информационной системе. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система. Перечень типов объектов защиты информационной системы. Требования к мерам и средствам защиты информации, применяемым в информационной системе.	1	36	Требования к мерам и средствам защиты информации
4	Разработка проектных решений по системе защиты информации информационной	Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления	1	36	Проектные решения по системе защиты информации

	системы	базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа). Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Организационные меры, виды и типы средств защиты информации. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.			информационной системы
5	Эксплуатационная документация на систему защиты информации информационной системы	Организационная структура системы защиты информации информационной системы. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы. Порядок контроля за событиями и действиями пользователей в информационной системе. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления	1	35	Эксплуатационная документация на систему защиты

		работоспособности в случае нарушения функционирования системы защиты информации информационной системы. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.			
6	Тестирование системы защиты информации информационной системы	Проверка работоспособности и совместимости средств защиты информации с информационными технологиями и техническими средствами обработки информации. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы. Корректировка документации на систему защиты информации информационной системы (при необходимости).	1	36	Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы.
7	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.	1	36	Раздел отчета. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
8	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).	0,5	18	Раздел отчета. Администрирование системы защиты информации информационной системы.

		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.			
9	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 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).	0,5	18	Раздел отчета. Реагирование на инциденты, связанные с нарушением требований о защите информации
10	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
11	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	0,5	18	Раздел отчета. Управление защитой информации

		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 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.			в информационной системе

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. Оценка возможностей и потенциала нарушителей (внешних, внутренних).
2. Анализ возможных уязвимостей информационной системы.
3. Возможные последствия от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

4. Физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами,
5. Режимы обработки информации в информационной системе в целом и в ее отдельных сегментах.
6. Модель угроз безопасности информации.
7. Определение значимости обрабатываемой информации конфиденциального характера.
8. Масштаб информационной системы.
9. Класс защищенности.
10. Цель и задачи обеспечения защиты информации в информационной системе.
11. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
12. Перечень типов объектов защиты информационной системы.
13. Требования к мерам и средствам защиты информации, применяемым в информационной системе.
14. Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).
15. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации.
16. Содержание состава мер по защите информации в соответствии с установленным классом защищенности информационной системы.
17. Организационные меры, виды и типы средств защиты информации.
18. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы.
19. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
20. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию) актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.
21. Организационная структура системы защиты информации информационной системы.
22. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации.
23. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы.
24. Порядок контроля за событиями и действиями пользователей в информационной системе.
25. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе.
26. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы.

27. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования.
28. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления работоспособности в случае нарушения функционирования системы защиты информации информационной системы.
29. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения.
30. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.
31. Проверка работоспособности и совместимости средств защиты информации с информационными технологиями и техническими средствами обработки информации.
32. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы.
33. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
34. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
35. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
36. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
37. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
38. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
39. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
40. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
41. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
42. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
43. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
44. 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).

45. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
46. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
47. 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
48. Выполнение организационных мер по защите информации.
49. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
50. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
51. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
52. 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.
53. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
54. 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).
55. 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.

10. 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 10.03.01 «Информационная безопасность».

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

Программа утверждена на заседании кафедры «Информационная безопасность» «29» августа 2020 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»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПОПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

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

Составители:

проф., к.т.н. Федоров Н.В.

Москва, 2020 год

1. Паспорт фонда оценочных средств

Таблица 1

производственная практика					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	**уметь:** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -настройка и обслуживание программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; Повышенный уровень: установка, настройка и обслуживание программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;	**знать:** программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; **уметь:** применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - применение программных средств системного, прикладного и специального назначения, инструментальные средств Повышенный уровень: - применение языков и систем программирования для решения профессиональных задач

ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты;	**уметь:** администрировать подсистемы информационной безопасности объекта защиты;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - администрирование подсистемы информационной безопасности объекта защиты; Повышенный уровень: - администрирование системы информационной безопасности объекта защиты;

ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;	**знать:** политики информационной безопасности; **уметь:** проводить реализацию политики информационной безопасности, **владеть:** комплексным подходом к обеспечению информационной безопасности объекта защиты;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - участие в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; Повышенный уровень: - участие в работах по разработке и реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	**уметь:** принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - участие сопровождении аттестации объекта информатизации по требованиям безопасности информации Повышенный уровень: -участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	**уметь:** принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-ппаратных и технических средств защиты информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - участие в проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации Повышенный уровень: участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;	**знать:** исходные данные для проектирования подсистем и средств обеспечения информационной безопасности; **уметь:** проводить технико-экономического обоснования соответствующих проектных решений; **владеть:** методами анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и технико-экономического обоснования соответствующих проектных решений;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности Повышенный уровень: - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	**знать:** техническую документацию с учетом действующих нормативных и методических документов; **уметь:** оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; Повышенный уровень: - разрабатывать и оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;

2. Оценочные средства для текущей аттестации

Отчет по практике

Отчет о практике должен содержать:

1. Определение актуальных угроз безопасности информации и разработку на их основе модели угроз.
2. Классификация информационной системы.
3. Определение требований к системе защиты информации информационной системы.
4. Разработка проектных решений по системе защиты информации информационной системы.
5. Эксплуатационная документация на систему защиты информации информационной системы.
6. Тестирование системы защиты информации информационной системы.
7. Обеспечение безопасности среды эксплуатации информационной системы
8. Администрирование системы защиты информации информационной системы.
9. Реагирование на инциденты, связанные с нарушением требований о защите информации.
10. Управление конфигурацией системы защиты информации автоматизированной системы
11. Управление защитой информации в информационной системе

3. Оценочные средства для промежуточной аттестации

Дифференцированный зачет
Вопросы для дифференцированного зачета

1. Оценка возможностей и потенциала нарушителей (внешних, внутренних).
2. Анализ возможных уязвимостей информационной системы.
3. Возможные последствия от реализации угроз безопасности информации для нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
4. Физические, функциональные и технологические взаимосвязи между сегментами (составными частями) информационной системы и взаимосвязи с иными информационными системами,
5. Режимы обработки информации в информационной системе в целом и в ее отдельных сегментах.
6. Модель угроз безопасности информации.
7. Определение значимости обрабатываемой информации конфиденциального характера.
8. Масштаб информационной системы.
9. Класс защищенности.
10. Цель и задачи обеспечения защиты информации в информационной системе.

11. Организация контролируемой зоны, в пределах которой размещаются стационарные технические средства, обрабатывающие информацию конфиденциального характера.
12. Средства защиты информации, а также средства, обеспечивающие функционирование информационной системы.
13. Контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
14. Защита технических средств, средств защиты информации и средств обеспечения функционирования.
15. Заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе.
16. Управление средствами защиты информации в информационной системе, включая восстановление их работоспособности, генерацию, смену и восстановление паролей.
17. Централизованное управление системой защиты информации автоматизированной системы (в случае технической возможности).
18. Информирование пользователей о правилах эксплуатации системы защиты информации автоматизированной системы и отдельных средств защиты информации и их обучение.
19. Выявление инцидентов, связанных с нарушением требований о защите информации, включая выявление сбоев в работе технических средств, программного обеспечения и средств защиты информации.
20. Выявление внедрения вредоносных компьютерных программ (вирусов), неправомерных действий пользователей и иных событий, связанных с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности).
21. Выявление причин возникновения инцидентов, связанных с нарушением требований о защите информации.
22. 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).
23. Обеспечение целостности системы защиты информации информационной системы, включая резервирование средств защиты информации.
24. Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых их разработчиками.
25. 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
26. Выполнение организационных мер по защите информации.

27. Контроль состояния защиты информации в информационной системе, включая контроль за событиями и действиями пользователей информационной системы.
28. Анализ и оценка функционирования системы защиты информации информационной системы, включая выявление и устранение недостатков в функционировании системы защиты информации информационной системы.
29. Периодический анализ уязвимостей информационной системы и оперативное принятие первоочередных мер по устранению вновь выявленных уязвимостей, приводящих к возникновению актуальных угроз безопасности.
30. 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.
31. Анализ влияния на систему защиты информации информационной системы планируемых изменений в информационной системе.
32. 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).
33. Сопровождение системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее.
34. Перечень нормативных правовых актов, методических документов и национальных стандартов, требованиям которых должна соответствовать информационная система.
35. Перечень типов объектов защиты информационной системы.
36. Требования к мерам и средствам защиты информации, применяемым в информационной системе.
37. Субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа).
38. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации.
39. Содержание состава мер по защите информации в соответствии с установленным классом защищенности информационной системы.
40. Организационные меры, виды и типы средств защиты информации.
41. Логическая структура, состав (количество) и места размещения элементов системы защиты информации автоматизированной системы.
42. Средства защиты информации с учетом их совместимости с информационными технологиями и техническими средствами обработки информации, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы.
43. Параметры настройки средств защиты информации, обеспечивающие реализацию мер по защите информации и блокирование (нейтрализацию)

актуальных угроз безопасности информации, в том числе путем устранения возможных уязвимостей информационной системы.

44. Организационная структура системы защиты информации информационной системы.
45. Состав, номенклатуру, места установки и параметры настройки средств защиты информации, программного обеспечения и технических средств обработки информации.
46. Порядок создания, удаления в информационной системе учетных записей пользователей и установления полномочий пользователей и администраторов информационной системы.
47. Порядок контроля за событиями и действиями пользователей в информационной системе.
48. Порядок обновления программного обеспечения, включая программное обеспечение средств защиты информации, в информационной системе.
49. Порядок выявления и устранения недостатков в системе защиты информации информационной системы, а также порядок внесения изменений в эксплуатационную документацию на систему защиты информации информационной системы.
50. Порядок контроля целостности системы защиты информации информационной системы и ее тестирования.
51. Правила эксплуатации системы защиты информации информационной системы, порядок ее настройки и восстановления работоспособности в случае нарушения функционирования системы защиты информации информационной системы.
52. Порядок управления параметрами настройки средств защиты информации, составом и конфигурацией технических средств обработки информации и программного обеспечения, а также контроля за несанкционированными подключениями технических средств обработки информации и установкой программного обеспечения.
53. Порядок архивирования информации конфиденциального характера, содержащейся в информационной системе, и стирания (уничтожения) данных и остаточной информации с машинных носителей информации и (или) уничтожения машинных носителей информации.
54. Проверка работоспособности и совместимости средств защиты информации с информационными технологиями и техническими средствами обработки информации.
55. Проверка выполнения средствами защиты информации требований к системе защиты информации информационной системы.