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

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

РАБОЧАЯ ПРОГРАММА
технологической практики

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2022

Москва 2022 г.

Разработчик(и):

доцент, к.т.н. 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 прохождения практики

К **основным целям** освоения технологической 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.

К **основным задачам** освоения технологической 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.

Компетенции обучающегося, формируемые в результате прохождения практики

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

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	ИПК-1.1. Знает современные виды информационного взаимодействия и обслуживания, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные сети и системы передачи информации, основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования, принципы построения криптографических алгоритмов; ИПК-1.2. Умеет использовать и настраивать программно-аппаратные средства защиты информации, проводить анализ показателей качества сетей и систем связи ИПК-1.3. Владеет навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ИОПК-7.1. Знает современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач, базовые структуры данных, основные алгоритмы сортировки и поиска и способы их эффективной реализации, основы администрирования операционных систем и

	вычислительных сетей, эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; ИОПК-7.2. Умеет выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные, формализовать поставленную задачу, выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах, устанавливать и осуществлять первичную настройку одной из операционных систем; ИОПК-7.3. Владеет навыками разработки программ на языке программирования высокого уровня, способами оценки сложности работы алгоритмов, основными подходами к организации процесса разработки программного обеспечения.
ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИОПК-1.2.1.Знает принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах; ИОПК-1.2.2.Умеет развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; ИОПК-1.2.3.Владеет навыками использования типовых криптографических алгоритмов
ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ИОПК-1.1.1. Знает формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; ИОПК-1.1.2. Умеет применять формальные модели для разработки политик безопасности, политик управления доступом; ИОПК-1.1.3. Владеет навыками создания формальных моделей управления доступом.
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.1 Знает информационно-коммуникационные технологии, программные средства системного и прикладного назначения; ИОПК-2.2. Умеет применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности ИОПК-2.3.Владеет навыками применения информационно-коммуникационных технологий, программными средствами системного и прикладного назначения, в том числе отечественного производства, для решения задач.
ПК-3. Способен принимать участие в организации и проведении контрольных проверок	ИПК-3.1. Знает методы и средства контроля эффективности технической защиты информации;

работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; ИПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.
ПК-4. Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ИПК-4.1. Знает свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления, задачи органов защиты информации на предприятиях, порядок организации работы и нормативные правовые акты по сертификации средств защиты информации; ИПК-4.2. Умеет квалифицированно исследовать состав документации предприятия (организации), разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; владеет методами формирования требований по защите информации.

2. Место практики в структуре образовательной программы

Технологическая практика относится к блоку 2 «Практики» части, формируемой участниками образовательных отношений (Б2.2), основной образовательной программы (Б2.2.1).

Практика базируется на дисциплинах базовой и вариативной части учебного плана.

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 8 семестре на базе предприятий требуемого профиля.

4. Структура и содержание практики

Общая трудоемкость практики составляет 9 зачетных единиц, 288 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 системы	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). 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	1	36	Проектные решения по системе защиты информации информационной 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.			
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 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,	1	35	Эксплуатационная документация на систему защиты

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

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

		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.			

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

1. 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

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».

7. Методические рекомендации

7.1 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.

7.2 Методические указания для обучающихся по освоению дисциплины

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.

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.

8.3 Оценочные средства

8.3.1 Текущий контроль

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

8.3.2 Промежуточная аттестация

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.