



**Автономная некоммерческая организация высшего образования
«Институт государственного администрирования»**

Центр дополнительного профессионального образования

ПРИНЯТА
Ученым советом АНО ВО «ИГА»
Протокол № 2
от «26» февраля 2026 года

УТВЕРЖДАЮ
Ректор АНО ВО «ИГА»
_____ А.В. Тараканов
«26» февраля 2026г.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ
«КИБЕРБЕЗОПАСНОСТЬ»**

Квалификация – ««Специалист по безопасности компьютерных систем и сетей»» (362 часа)

Автор: зав. каф. «Математики и ИТ» Малыш А.Е.

Москва 2026 г.

Общая характеристика программы

Цель программы: формирование у слушателей комплексных знаний и практических навыков в области администрирования и обеспечения бесперебойной работы информационно-коммуникационных систем и ИТ-инфраструктуры организации.

Программа направлена на развитие компетенций, необходимых для:

- эффективного мониторинга, диагностики и устранения неполадок в работе ИТ-сервисов;
- обеспечения требуемого уровня надёжности, доступности и безопасности ИТ-систем (в т.ч. соблюдения параметров SLA, RTO, RPO);
- оптимизации использования ИТ-ресурсов (серверного оборудования, СХД, сетевых ресурсов, лицензий ПО, облачных сервисов) с учётом текущих и перспективных потребностей организации;
- внедрения современных методов автоматизации администрирования и развёртывания инфраструктуры (в т.ч. с применением инструментов Infrastructure as Code — Ansible, Terraform и др.);
- планирования и реализации мероприятий по масштабированию, модернизации и аварийному восстановлению ИТ-сервисов;
- ведения актуальной технической и эксплуатационной документации, регламентирующей работу ИТ-инфраструктуры.

В результате освоения программы слушатели смогут обеспечивать стабильную и эффективную работу ИТ-систем, минимизировать риски простоев и потери данных, а также способствовать повышению общей операционной эффективности организации за счёт грамотного управления ИТ-ресурсами.

При разработке программы использованы следующие профессиональные стандарты:

Код профессионального стандарта по классификации Минтруда	Вид профессиональной деятельности	Наименование профессионального стандарта (с последующими изменениями и дополнениями)	Уровень (подуровень) квалификации
ПС 06.032 «Специалист по безопасности компьютерных систем и сетей» — приказ Минтруда № 536н от 14.09.2022	«Защита информации в компьютерных системах и сетях»	Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (код 06.032), утверждённый приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 536н, с последующими изменениями и дополнениями	Уровень (подуровень) квалификации: 6

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения программы:

В результате освоения программы слушатели должны приобрести и совершенствовать следующие профессиональные компетенции:

В области управления и организации ИБ:

- анализировать угрозы информационной безопасности и определять актуальные риски для информационных систем организации;
- разрабатывать, внедрять и актуализировать организационно-распорядительную документацию по защите информации (политики, регламенты, инструкции);
- участвовать в построении и сопровождении системы менеджмента информационной безопасности в соответствии с требованиями ISO 27001 и российского законодательства (№ 149-ФЗ, № 152-ФЗ, № 187-ФЗ);
- проводить внутренний аудит ИБ и оценивать соответствие требованиям регуляторов (ФСТЭК России, ФСБ России, Роскомнадзор);
- применять методики оценки рисков, планировать и обосновывать меры защиты.

В области технической защиты:

- применять криптографические методы защиты информации: симметричное и асимметричное шифрование, электронную подпись, хэширование;
- администрировать межсетевые экраны, системы обнаружения/предотвращения вторжений (IDS/IPS), VPN-шлюзы;
- защищать веб-приложения и API от типовых атак (SQL-инъекции, XSS, CSRF), применять методы безопасной разработки;
- обеспечивать защиту данных: разграничение доступа, шифрование данных в покое и при передаче, резервное копирование и восстановление;
- защищать персональные данные и информацию ограниченного доступа в соответствии с законодательством РФ;
- обеспечивать безопасность облачных сервисов и инфраструктуры (IaaS, PaaS, SaaS).

В области реагирования на инциденты:

- выявлять, классифицировать и регистрировать инциденты информационной безопасности;
- проводить первичный анализ и реагирование на инциденты, выполнять сбор и сохранение цифровых улик;
- восстанавливать работоспособность информационных систем после атак и сбоев;
- осуществлять мониторинг и анализ защищённости, проводить тестирование на проникновение в рамках согласованного регламента.

В области работы с персоналом:

- разрабатывать и проводить обучающие мероприятия по информационной безопасности для сотрудников;
- выявлять и противодействовать атакам социальной инженерии, проводить

- антифишинговые тренировки;
- формировать культуру информационной безопасности в организации.

В области современных технологий:

- применять средства автоматизации, машинного обучения и ИИ-инструменты для повышения эффективности защиты;
- оценивать перспективные технологии (блокчейн, квантовая криптография) с точки зрения рисков и возможностей для ИБ.

Планируемые результаты обучения по программе По итогам освоения программы слушатели должны:

Знать:

- понятийный аппарат информационной безопасности: свойства безопасности информации (конфиденциальность, целостность, доступность), модель угроз, модель нарушителя;
- историю и современное состояние отрасли ИБ, актуальные угрозы и векторы атак;
- нормативную правовую базу в области защиты информации: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 98-ФЗ, требования ФСТЭК России и ФСБ России, подзаконные акты в области КИИ и персональных данных;
- международные и национальные стандарты в области ИБ (ISO/IEC 27001, ГОСТ Р ИСО/МЭК серии 27000, руководящие документы ФСТЭК);
- принципы построения системы менеджмента информационной безопасности, процессы и процедуры СУИБ;
- основные криптографические методы защиты информации: симметричное и асимметричное шифрование, хэширование, электронную подпись, основы криптостойкости;
- архитектуру защищённых сетей, принципы работы межсетевых экранов, IDS/IPS, VPN-технологий;
- типовые уязвимости веб-приложений (SQL-инъекции, XSS, CSRF) и методы безопасной разработки программного обеспечения;
- методы и средства защиты данных: разграничение доступа, шифрование в покое и при передаче, резервное копирование, восстановление после сбоев;
- модели облачных услуг (IaaS, PaaS, SaaS) и требования к защите данных в облачной инфраструктуре;
- порядок организации работ по инцидент-менеджменту: классификацию инцидентов, порядок реагирования, основы цифровой криминалистики;
- психологические приёмы и методы социальной инженерии, признаки фишинговых атак;
- перспективные направления развития ИБ: применение искусственного интеллекта и машинного обучения, блокчейн-технологии, квантовую криптографию;
- требования к обработке персональных данных и меры по их обеспечению согласно № 152-ФЗ.

Уметь:

- анализировать угрозы информационной безопасности и оценивать актуальные риски для информационных систем организации;
- разрабатывать и актуализировать организационно-распорядительную документацию по защите информации (политики безопасности, регламенты, инструкции);
- применять методики оценки рисков и выбирать меры защиты в соответствии с их уровнем;
- проводить аудит информационной безопасности и оценивать соответствие требованиям стандартов и регуляторов;
- применять криптографические средства защиты: настраивать шифрование, использовать электронную подпись, контролировать целостность данных;
- администрировать средства защиты сетевой инфраструктуры: межсетевые экраны, системы обнаружения вторжений, VPN-шлюзы;
- выявлять и устранять типовые уязвимости веб-приложений, применять методы защищённого программирования;
- обеспечивать управление доступом к данным и их защиту на всех этапах жизненного цикла;
- организовывать резервное копирование и восстановление информационных систем после сбоев и атак;
- выявлять, регистрировать и классифицировать инциденты информационной безопасности, участвовать в их расследовании;
- противодействовать атакам социальной инженерии, проводить обучение персонала и антифишинговые тренировки;
- применять инструменты мониторинга и анализа защищённости, автоматизировать процессы защиты.

Общие требования по программе

Требования к уровню образования слушателей	– лица, имеющие среднее профессиональное образование, высшее образование – бакалавриат, высшее образование – специалитет, магистратура
Срок обучения	трудоемкость программы 362 часа (9 з.е.), продолжительность обучения – 3 месяца
Форма обучения	очно-заочная с применением дистанционных образовательных технологий и электронного обучения
Режим занятий	не более 6 часов в день

УЧЕБНЫЙ ПЛАН
программы профессиональной переподготовки
«КИБЕРБЕЗОПАСНОСТЬ»

№ п/п	Наименование модуля	Трудоемкост ь		В том числе				Форма контроля
				Внеаудиторны е занятия			Самостоятельная работа*	
		В зачетных единицах	В часах	Всего	из них			
					Лекции*	Практические занятия		
1	Модуль 1. Основы информационной безопасности Модуль формирует понятийный аппарат дисциплины: свойства безопасности информации (конфиденциальность, целостность, доступность), модель угроз и модель нарушителя, классификацию актуальных атак. Слушатели знакомятся с историей отрасли, ключевыми векторами угроз современности и ролями участников рынка ИБ.	1	40	12	4	8	28	Зачет методом тестирования
2	Модуль 2. Нормативно-правовое регулирование в области защиты информации Рассматривается российская и международная правовая база: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 98-ФЗ, требования и методические документы ФСТЭК и ФСБ России. Отдельное внимание уделяется обязанностям операторов	1	40	12	4	8	28	Зачет методом тестирования

*С применением дистанционных образовательных технологий и электронного обучения

	персональных данных и субъектов критической информационной инфраструктуры.							
3	<p>Модуль 3. Управление информационной безопасностью и оценка рисков</p> <p>Модуль посвящён построению системы менеджмента ИБ по ISO/IEC 27001: разработке политики безопасности, организации процессов СУИБ, проведению внутреннего аудита. Слушатели осваивают методики оценки рисков и учатся обосновывать выбор мер защиты.</p>	1	40	12	4	8	28	Зачет методом тестирования
4	<p>Модуль 4. Криптографические методы защиты информации</p> <p>Изучаются основы криптографии: симметричное и асимметричное шифрование, хэширование, электронная подпись, управление ключами и сертификатами. Практическая часть включает применение российских криптостандартов (ГОСТ) и сервисов ЭП в реальных задачах.</p>	1	40	12	4	8	28	Зачет методом тестирования
5	<p>Модуль 5. Безопасность сетевой инфраструктуры</p> <p>Разбирается архитектура защищённых сетей: сегментирование, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), VPN-технологии. Слушатели получают навыки администрирования средств сетевой защиты и анализа сетевого трафика.</p>	1	40	12	4	8	28	Зачет методом тестирования
6	<p>Модуль 6. Безопасность веб-приложений и защищённая разработка</p> <p>Модуль охватывает типовые</p>	1	40	12	4	8	28	Зачет методом тестирования

	уязвимости веб-приложений (SQL-инъекции, XSS, CSRF) и практики безопасной разработки (SDLC, OWASP Top 10). В ходе практикума слушатели выявляют уязвимости в учебных приложениях и устраняют их средствами защищённого программирования.							
7	Модуль 7. Защита данных: персональные данные, облака и резервирование Рассматриваются управление доступом, шифрование данных в покое и при передаче, построение систем резервного копирования и восстановления. Отдельные темы — обеспечение безопасности облачных сервисов (IaaS, PaaS, SaaS) и требования к обработке персональных данных.	1	40	12	4	8	28	Зачет методом тестирования
8	Модуль 8. Управление инцидентами информационной безопасности Модуль формирует навыки выявления, классификации и регистрации инцидентов ИБ, планирования реагирования и восстановления систем после атак. Включает основы цифровой криминалистики, противодействие социальной инженерии и организацию обучения персонала.	1	40	12	4	8	28	Зачет методом тестирования
9	Модуль 9. Современные технологии в обеспечении информационной безопасности Модуль знакомит с перспективными направлениями отрасли: применением искусственного интеллекта и машинного обучения в защите, блокчейн-технологиями и квантовой криптографией. Слушатели	1	40	12	4	8	28	Зачет методом тестирования

	оценивают новые технологии с точки зрения рисков и возможностей и осваивают средства автоматизации процессов ИБ.							
	Всего:	9	360	108	36	72	252	Зачет методом тестирования
	Итоговая аттестация		2					Экзамен методом тестирования
	Общая трудоемкость программы:	9	362	108	36	72	252	

Проректор по учебной работе АНО ВО «ИГА»
_____ П.Н. Рузанов

26 февраля 2026 г.

Учебно-ТЕМАТИЧЕСКИЙ план
программы профессиональной переподготовки
«КИБЕРБЕЗОПАСНОСТЬ»

№ п/п	Наименование дисциплины, модуля	Трудоемкость		В том числе					Форма контроля
		В зачетных единицах	В часах	Всего	из них: Лекции Практические занятия	Внеаудиторные занятия	Самостоятельная работа *		
	Модуль 1. Основы информационной безопасности								
1	Тема 1.1. Предмет, цели и задачи информационной безопасности		10	3	1	2		7	Зачет методом тестирования
2	Тема 1.2. Модель угроз и модель нарушителя		10	3	1	2		7	Диф. зачет методом тестирования
3	Тема 1.3. Актуальный ландшафт киберугроз		10	3	1	2		7	Зачет методом тестирования
4	Тема 1.4. Участники отрасли и инфраструктура безопасности		10	3	1	2		7	Диф. зачет методом тестирования
	Общая трудоемкость модуль 1		40	12	4	8		28	
	Модуль 2. Нормативно-правовое регулирование в области защиты информации								
5	Тема 2.1. Правовая база защиты информации в РФ		10	3	1	2		7	Зачет методом тестирования
6	Тема 2.2. Требования ФСТЭК и ФСБ России		10	3	1	2		7	Диф. зачет методом тестирования

									я
7	Тема 2.3. Персональные данные: права субъектов и обязанности операторов		10	3	1	2		7	Зачет методом тестировани я
8	Тема 2.4. Международное регулирование и отраслевые стандарты		10	3	1	2		7	Диф. зачет методом тестировани я
Общая трудоемкость модуль 2			40	12	4	8		28	
Модуль 3. Управление информационной безопасностью и оценка рисков									
9	Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001		10	3	1	2		7	Зачет методом тестировани я
10	Тема 3.2. Политика безопасности и организационно- распорядительная документация		10	3	1	2		7	Диф. зачет методом тестировани я
11	Тема 3.3. Оценка и управление рисками ИБ		10	3	1	2		7	Зачет методом тестировани я
12	Тема 3.4. Внутренний аудит и анализ защищённости		10	3	1	2		7	Диф. зачет методом тестировани я
Общая трудоемкость модуль 3			40	12	4	8		28	
Модуль 4. Криптографические методы защиты информации									
13	Тема 4.1. Основы криптографии и симметричное шифрование		10	3	1	2		7	Зачет методом тестировани я
14	Тема 4.2. Асимметричная криптография и электронная подпись		10	3	1	2		7	Диф. зачет методом тестировани я
15	Тема 4.3. Хэширование, целостность и аутентификация данных		10	3	1	2		7	Зачет методом тестировани я
16	Тема 4.4. Управление ключами и инфраструктура открытых ключей		10	3	1	2		7	Диф. зачет методом тестировани я
Общая трудоемкость модуль 4			40	12	4	8		28	
Модуль 5. Безопасность сетевой инфраструктуры									
17	Тема 5.1. Архитектура защищённых сетей и сегментирование		10	3	1	2		7	Зачет методом тестировани я
18	Тема 5.2. Межсетевое экранирование и контроль трафика		10	3	1	2		7	Диф. зачет методом тестировани я
19	Тема 5.3. Обнаружение вторжений и анализ сетевых трафика		10	3	1	2		7	Зачет методом тестировани я
20	Тема 5.4. VPN- технологии и защищённый удалённый доступ		10	3	1	2		7	Диф. зачет методом тестировани я
Общая трудоемкость модуль 5			40	12	4	8		28	

	Модуль 6. Безопасность веб-приложений и защищённая разработка								
21	Тема 6.1. Типовые уязвимости веб-приложений		10	3	1	2		7	Зачет методом тестирования
22	Тема 6.2. Методы защищённой разработки ПО		10	3	1	2		7	Диф. зачет методом тестирования
23	Тема 6.3. Аутентификация, сессии и управление доступом в веб		10	3	1	2		7	Зачет методом тестирования
24	Тема 6.4. Практикум: поиск и устранение уязвимостей		10	3	1	2		7	Диф. зачет методом тестирования
	Общая трудоемкость модуль 6		40	12	4	8		28	
	Модуль 7. Защита данных: персональные данные, облака и резервирование								
25	Тема 7.1. Управление доступом и разграничение прав		10	3	1	2		7	Зачет методом тестирования
26	Тема 7.2. Шифрование данных в покое и при передаче		10	3	1	2		7	Диф. зачет методом тестирования
27	Тема 7.3. Резервное копирование и восстановление систем		10	3	1	2		7	Зачет методом тестирования
28	Тема 7.4. Безопасность облачных сервисов и ПДн		10	3	1	2		7	Диф. зачет методом тестирования
	Общая трудоемкость модуль 7		40	12	4	8		28	
	Модуль 8. Управление инцидентами информационной безопасности								
29	Тема 8.1. Организация процесса реагирования на инциденты		10	3	1	2		7	Зачет методом тестирования
30	Тема 8.2. Инструменты мониторинга и SIEM		10	3	1	2		7	Диф. зачет методом тестирования
31	Тема 8.3. Основы цифровой криминалистики		10	3	1	2		7	Зачет методом тестирования
32	Тема 8.4. Человеческий фактор и обучение персонала		10	3	1	2		7	Диф. зачет методом тестирования
	Общая трудоемкость модуль 8		40	12	4	8		28	
	Модуль 9. Современные технологии в обеспечении информационной безопасности								
33	Тема 9.1. Искусственный интеллект и машинное обучение в ИБ		10	3	1	2		7	Зачет методом тестирования
34	Тема 9.2. Блокчейн-технологии и безопасность распределённых систем		10	3	1	2		7	Диф. зачет методом тестирования

35	Тема 9.3. Квантовая криптография и постквантовые алгоритмы		10	3	1	2		7	Зачет методом тестирования
36	Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта		10	3	1	2		7	Диф. зачет методом тестирования
	Общая трудоемкость модуль 9		40	12	4	8		28	
	Всего:		360	108	36	72		252	
	Итоговая аттестация		2						Экзамен методом тестирования
	Общая трудоемкость программы:		362						

* Самостоятельная работа включает проработку материалов лекций и выполнение практических заданий.

Рабочая программа учебного курса «КИБЕРБЕЗОПАСНОСТЬ»

Курс состоит из 9 учебных модулей:

Модуль 1. Основы информационной безопасности

Модуль 2. Нормативно-правовое регулирование в области защиты информации

Модуль 3. Управление информационной безопасностью и оценка рисков

Модуль 4. Криптографические методы защиты информации

Модуль 5. Безопасность сетевой инфраструктуры

Модуль 6. Безопасность веб-приложений и защищённая разработка

Модуль 7. Защита данных: персональные данные, облака и резервирование

Модуль 8. Управление инцидентами информационной безопасности

Модуль 9. Современные технологии в обеспечении информационной безопасности

Рабочая программа Модуля 1.
«Основы информационной безопасности»
Учебно-тематический план модуля 1

№ п/п	Наименование дисциплины, модуля	Трудоемкост ь В том числе					Самосто ятельная работа*	Форма контроля
		В зачет ных едини цах.	В часа х	Всег о	из них			
					Лек ции *	Практи ческие заняти я		
Модуль 1. Основы информационной безопасности								
1	Тема 1.1. Предмет, цели и задачи информационной безопасности		10	3	1	2	7	Зачет методом тестирования
2	Тема 1.2. Модель угроз и модель нарушителя		10	3	1	2	7	Диф. зачет методом тестирования
3	Тема 1.3. Актуальный ландшафт киберугроз		10	3	1	2	7	Зачет методом тестирования
4	Тема 1.4. Участники отрасли и инфраструктура безопасности		10	3	1	2	7	Диф. зачет методом тестирования
	Общая трудоемкость модуля 1		40	12	4	8	28	

Содержание модуля 1

Тема 1.1. Предмет, цели и задачи информационной безопасности.

Понятие информационной безопасности и информационной безопасности организации. Базовые свойства информации: конфиденциальность, целостность, доступность (триада КЦД). Цели и задачи обеспечения информационной безопасности. Виды угроз информационной безопасности: преднамеренные и непреднамеренные, внутренние и внешние. Объекты защиты информации и категории обрабатываемых сведений: общедоступная информация, персональные данные (152-ФЗ), конфиденциальная информация, коммерческая тайна, государственная тайна. Понятие информационной безопасности как процесса: непрерывность, системность, комплексность. Правовые основы информационной безопасности: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Ответственность за нарушения в области защиты информации.

Тема 1.2. Модель угроз и модель нарушителя.

Понятие модели угроз, её назначение и состав. Виды угроз: умышленные и неумышленные, внешние и внутренние, пассивные и активные. Уязвимость, атака, инцидент информационной безопасности. Уровни угроз и способы их оценки. Порядок разработки модели угроз по методике ФСТЭК России (приказ ФСТЭК России от 05.02.2021 № 239). Модель нарушителя: категории нарушителей (внутренние и внешние), их цели, мотивация, квалификация, доступ к информационным ресурсам, используемые инструменты. Ранжирование нарушителей по потенциалу. Связь модели угроз и модели нарушителя с выбором мер защиты. Актуализация модели угроз.

Тема 1.3. Актуальный ландшафт киберугроз.

Современные типы кибератак: вредоносное программное обеспечение (вирусы, черви, трояны, руткиты), фишинг и социальная инженерия, вымогательское ПО (ransomware), атаки с применением шифровальщиков. Целевые атаки (APT): этапы атак, каналы проникновения, закрепление в инфраструктуре. Атаки на цепочку поставок (supply chain). Атаки на промышленные системы и критическую информационную инфраструктуру. Компрометация деловой переписки (BEC), DDoS-атаки, утечки данных. Актуальные статистические данные по киберугрозам в России и мире. Основные векторы атак на организации: сотрудники, веб-приложения, периферийная инфраструктура, мобильные устройства.

Тема 1.4. Участники отрасли и инфраструктура безопасности.

Государственные регуляторы: ФСТЭК России, ФСБ России, Роскомнадзор, Минцифры России. Национальный координационный центр по компьютерным инцидентам (НКЦКИ), ГосСОПКА, ФинЦЕРТ Банка России. Лицензирование и сертификация средств защиты информации. Вендоры средств защиты информации: антивирусные средства, межсетевые экраны, SIEM, DLP, EDR/XDR. Системные интеграторы и дистрибьюторы. Корпоративные центры мониторинга и реагирования: SOC, MSSP, ИБ-специалисты организации (CISO, аналитик SOC, пентестер, администратор ИБ). Сообщество безопасности: bug bounty, CTF, конференции, профессиональные сертификации. Российский рынок средств защиты информации: импортозамещение, реестр отечественного ПО.

Содержание практических занятий

№ темы	Наименование темы, по которой предусмотрено практическое занятие	Формы и методы проведения
1.1.	Предмет, цели и задачи информационной безопасности	Выполнение практических заданий, обмен опытом
1.2.	Модель угроз и модель нарушителя	Выполнение практических заданий, обмен опытом
1.3.	Актуальный ландшафт киберугроз	Выполнение практических заданий, обмен опытом
1.4.	Участники отрасли и инфраструктура безопасности	Выполнение практических заданий, обмен опытом

Рекомендуемый перечень практических заданий

Практические задания по теме 1.1 «Предмет, цели и задачи информационной безопасности»

Задание 1.

Составьте перечень информационных активов условной организации (документы, базы данных, системы). Для каждого актива определите, какие из свойств КЦД (конфиденциальность, целостность, доступность) являются критичными и обоснуйте вывод. Оформите результат в виде таблицы.

Задание 2.

Проведите классификацию информации в организации по категориям (общедоступная, персональные данные, коммерческая тайна). Для каждой категории укажите применимые нормативные требования и меры защиты. Сверьте классификацию с требованиями 149-ФЗ и 152-ФЗ.

Задание 3.

Разработайте краткий перечень целей и задач информационной безопасности для выбранной организации: определите, какие активы защищаются, от кого и от чего, с какими приоритетами. Оформите документ «Цели и задачи ИБ» объёмом 1–2 страницы.

Практические задания по теме 1.2 «Модель угроз и модель нарушителя»

Задание 1.

По методике ФСТЭК России (приказ № 239) определите объекты защиты и их уровни защищённости. Заполните форму исходных данных для разработки модели угроз: перечень объектов, категории обрабатываемой информации, наличие подключений к сети «Интернет».

Задание 2.

Разработайте модель нарушителя для условной организации: определите 2–3 категории нарушителей (внешний злоумышленник, недобросовестный сотрудник, подрядчик), их цели, мотивацию, квалификацию и доступ к ресурсам. Оформите в виде таблицы «Категория — Цель — Мотивация — Квалификация — Потенциал».

Задание 3.

Постройте карту актуальных угроз для выбранной организации: отнесите каждую угрозу к типу (внешняя/внутренняя, умышленная/неумышленная), оцените вероятность и ущерб, разместите угрозы в матрице рисков 3×3 и предложите по 1–2 меры защиты для наиболее критичных угроз.

Практические задания по теме 1.3 «Актуальный ландшафт киберугроз»

Задание 1.

Составьте обзор актуальных киберугроз за последний квартал на основе публичных отчётов вендоров и сообщений НКЦКИ: выделите 5 наиболее распространённых типов атак, укажите отрасли-мишени и типичные векторы проникновения. Оформите аналитическую записку.

Задание 2.

Разберите реальный кейс атаки вымогательского ПО (ransomware): опишите сценарий атаки по этапам (первичное проникновение, закрепление, распространение, шифрование, вымогательство), определите, какие меры защиты могли бы прервать атаку на каждом этапе.

Задание 3.

Смоделируйте фишинговую атаку на сотрудника: составьте признаки фишингового письма, разберите реальный пример, разработайте краткий алгоритм

действий сотрудника при подозрении на фишинг и чек-лист проверки входящих сообщений.

Практические задания по теме 1.4 «Участники отрасли и инфраструктура безопасности»

Задание 1.

Составьте схему взаимодействия организации с регуляторами при инцидентах: кто, когда и по какой форме обязан уведомлять НКЦКИ, Роскомнадзор, ФинЦЕРТ. Оформите в виде пошаговой инструкции для дежурной смены.

Задание 2.

Сравните модели построения корпоративной защиты: собственный SOC, аутсорсинг (MSSP) и гибридная модель. Сопоставьте их по стоимости, скорости реагирования, глубине экспертизы и требованиям к персоналу. Обоснуйте выбор модели для небольшой и крупной организации.

Задание 3.

Изучите состав типового набора средств защиты информации (антивирус, МСЭ, EDR, DLP, SIEM): для каждого класса средств опишите назначение, место в архитектуре защиты и типовых российских вендоров из реестра отечественного ПО. Оформите сравнительную таблицу.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с конспектами лекций, решения практических задач, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд библиотеки и Интернет-ресурсы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и учебные материалы, разработанные профессорско-преподавательским составом, конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей. Преподаватель проводит офлайн консультацию слушателей для оценивания полноты и уровня самостоятельного освоения материала.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения и проводится в образовательной среде.

№	Наименование темы	Содержание самостоятельной работы
1.1	Тема 1.1. Предмет, цели и задачи информационной безопасности	Изучение основных понятий и терминологии информационной безопасности; анализ положений 149-ФЗ и 152-ФЗ; составление перечня информационных активов и определение их критичности по триаде КЦД; подготовка конспекта по целям и задачам ИБ организации.

1.2	Тема 1.2. Модель угроз и модель нарушителя	Изучение методики определения актуальных угроз (приказ ФСТЭК России № 239); разработка исходных данных для модели угроз условной организации; описание категорий нарушителей и их характеристик; составление матрицы рисков.
1.3	Тема 1.3. Актуальный ландшафт киберугроз	Мониторинг актуальных угроз на публичных ресурсах (отчёты вендоров, бюллетени НКЦКИ); разбор реальных кейсов атак (ransomware, фишинг, АРТ); подготовка аналитической записки об актуальных угрозах для отрасли организации.
1.4	Тема 1.4. Участники отрасли и инфраструктура безопасности	Изучение структуры государственных регуляторов и порядков уведомления об инцидентах; обзор российского рынка средств защиты информации и реестра отечественного ПО; сравнение моделей построения защиты (SOC, MSSP, гибрид); подготовка схемы взаимодействия с регуляторами.

Перечень вопросов для самостоятельной работы и промежуточной аттестации

Тема 1.1. Предмет, цели и задачи информационной безопасности

1. Что понимается под информационной безопасностью? Чем она отличается от защиты информации?
2. Назовите и охарактеризуйте три базовых свойства информации (триада КЦД).
3. Какие цели преследует обеспечение информационной безопасности организации?
4. Перечислите основные задачи информационной безопасности.
5. Какие виды угроз информационной безопасности существуют? Приведите классификацию.
6. Какие объекты защиты информации выделяют в организации?
7. Какие категории информации обрабатываются в организации и чем они регулируются?
8. В чём суть Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
9. Какая ответственность предусмотрена за нарушения в области защиты информации?
10. Почему информационную безопасность рассматривают как непрерывный процесс?

Тема 1.2. Модель угроз и модель нарушителя

1. Что такое модель угроз и для чего она разрабатывается?
2. Из каких элементов состоит модель угроз?
3. Чем умышленные угрозы отличаются от неумышленных?
4. Какие способы разработки модели угроз предусмотрены методикой ФСТЭК России?

5. Что регулирует приказ ФСТЭК России от 05.02.2021 № 239?
6. Что такое модель нарушителя и из каких компонентов она состоит?
7. Какие категории нарушителей выделяют? По каким признакам их классифицируют?
8. Как нарушители ранжируются по потенциалу?
9. Как модель угроз и модель нарушителя связаны с выбором мер защиты?
10. Когда и как проводится актуализация модели угроз?

Тема 1.3. Актуальный ландшафт киберугроз

1. Какие основные типы вредоносного программного обеспечения существуют?
2. В чём заключается фишинг и социальная инженерия? Приведите примеры.
3. Что такое вымогательское ПО (ransomware) и каков типовой сценарий атаки с его применением?
4. Что такое целевая атака (APT) и какие этапы она включает?
5. Что такое атака на цепочку поставок (supply chain)?
6. Чем опасны атаки на критическую информационную инфраструктуру?
7. Что такое компрометация деловой переписки (BEC)?
8. Какие основные векторы атак на организации существуют?
9. Какова текущая статистика киберугроз в России и мире?
10. Какие источники информации об актуальных угрозах вы знаете?

Тема 1.4. Участники отрасли и инфраструктура безопасности

1. Какие государственные органы регулируют сферу информационной безопасности в России?
2. Каковы функции ФСТЭК России в области информационной безопасности?
3. Что такое НКЦКИ и какова его роль при инцидентах?
4. Что такое ГосСОПКА и кто в неё входит?
5. Каков порядок лицензирования деятельности в области защиты информации?
6. Как средства защиты информации проходят сертификацию?
7. Какие классы средств защиты информации используют вендоры? Перечислите основные классы (антивирус, МСЭ, SIEM, DLP, EDR).
8. Что такое SOC и какие модели его построения существуют?
9. Какие специалисты работают в области информационной безопасности и каковы их роли?
10. Что такое реестр отечественного ПО и почему он важен для информационной безопасности?

Литература

Основная литература:

Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: учебное пособие. — М.: РИОР: ИНФРА-М, 2023. — 336 с.

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. — М.: ФОРУМ: ИНФРА-М, 2022. — 416 с.

Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие. — М.: ФОРУМ: ИНФРА-М, 2022. — 368 с.

Мельников В. П., Клейменов С. В., Петраков А. М. Информационная безопасность: учебник. — М.: Академия, 2021. — 336 с.

Дополнительная литература:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Приказ ФСТЭК России от 05.02.2021 № 239 «Об утверждении Методики оценки угроз безопасности информации».

ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, кибербезопасность и защита информации. Системы менеджмента информационной безопасности. Требования.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

Интернет-ресурсы:

Официальный сайт ФСТЭК России — www.fstec.ru.

Официальный портал персональных данных — pd.rkn.gov.ru.

Официальный интернет-портал правовой информации — pravo.gov.ru.

Госуслуги. Информационная безопасность — www.gosuslugi.ru.

Бюллетени и рекомендации НКЦКИ — www.cert.su.ru.

Рабочая программа Модуля 2.

«Нормативно-правовое регулирование в области защиты информации»

Учебно-тематический план модуля 2

№ п/п	Наименование дисциплины, модуль	Трудоемкость, в часах	Внеаудиторные занятия	В том числе	Форма контроля

		я, темы						
			Всего	Самостоятельная работа	Всего		Практические занятия	
Модуль 2. Нормативно-правовое регулирование в области защиты информации								
1	Тема 2.1. Правовая база защиты информации в РФ	10	3	1	2	7	Зачет методом тестирования	
2	Тема 2.2. Требования ФСТЭК и ФСБ России	10	3	1	2	7	Диф. зачет методом тестирования	
3	Тема 2.3. Персональные данные: права субъектов и обязанности операторов	10	3	1	2	7	Зачет методом тестирования	
4	Тема 2.4. Международное регулирование и отраслевые	10	3	1	2	7	Диф. зачет методом тестирования	

	стандарты							
Общая трудоемкость модуля 2		1	40	12	4	8	28	

Содержание модуля 2

Тема 2.1. Правовая база защиты информации в РФ

Иерархия нормативных актов в области защиты информации: Конституция РФ (ст. 29, ч. 4), федеральные конституционные и федеральные законы, подзаконные акты. Понятие информации, информационных технологий и информационной безопасности по 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Категории информации по доступности: общедоступная информация, информация ограниченного доступа, конфиденциальная информация, государственная тайна (98-ФЗ «О коммерческой тайне», закон РФ «О государственной тайне»).

Отраслевые требования к защите информации: 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ)», требования к защите информации, персональные данные (152-ФЗ «О персональных данных»).

Ответственность за нарушения в области защиты информации: ст. 272–274 УК РФ (несанкционированный доступ, создание вредоносных программ, нарушение правил эксплуатации), статьи КоАП РФ (ст. 13.11, 13.12), гражданско-правовая ответственность за утечки.

Государственные органы в области защиты информации: ФСТЭК России, ФСБ России, Роскомнадзор, Генеральная прокуратура РФ — функции, полномочия, зоны ответственности.

Тема 2.2. Требования ФСТЭК и ФСБ России

ФСТЭК России: функции по технической защите информации, лицензирование, сертификация средств защиты информации, государственный контроль.

Приказы ФСТЭК России: № 17 (защита информации в государственных информационных системах), № 21 (защита персональных данных в ИСПДн), № 239 (защита информации в значимых объектах КИИ), № 31 (требования к средствам защиты).

ФСБ России: функции в области шифрования (СКЗИ), криптографической защиты информации, лицензирование в области СКЗИ, требования к аттестации объектов информатизации.

Модели безопасности и уровни защищённости: классы защищённости информационных систем (УЗ1–УЗ4), уровни защищённости персональных данных (УЗ1–УЗ4 по 152-ФЗ), категории значимости объектов КИИ.

Аттестация объектов информатизации: требования, порядок проведения аттестации, документы аттестации, сроки действия.

Тема 2.3. Персональные данные: права субъектов и обязанности операторов

152-ФЗ «О персональных данных»: понятие персональных данных, категории (общедоступные, специальные, биометрические), обработка и её цели.

Права субъектов персональных данных: право на доступ к своим данным, право на уточнение, блокирование, уничтожение данных, право на отзыв согласия, право на обжалование действий оператора.

Обязанности операторов персональных данных: получение согласия субъекта, уведомление Роскомнадзора, локализация баз данных на территории РФ, меры по защите ПДн, реагирование на инциденты.

Особенности обработки ПДн: трансграничная передача данных, обработка ПДн в системах государственного и муниципального управления, обезличивание данных.

Ответственность за утечки персональных данных: 270-ФЗ (административная ответственность), 420-ФЗ (уголовная ответственность за незаконный оборот ПДн), компенсация морального вреда.

Тема 2.4. Международное регулирование и отраслевые стандарты

Будапештская конвенция о киберпреступности: основные положения, протоколы, международное сотрудничество в борьбе с киберпреступностью.

GDPR (Общий регламент по защите данных ЕС): основные принципы, права субъектов данных, обязанности контролёров и обработчиков, штрафы, различия и сходства с 152-ФЗ.

Международные стандарты информационной безопасности: ISO/IEC 27001 (системы менеджмента ИБ), ISO/IEC 27002 (меры контроля), NIST CSF (рамки кибербезопасности).

Отраслевые стандарты: PCI DSS (безопасность платёжных карт), SWIFT CSP, ГОСТ Р 57580 (безопасность финансовых операций), отраслевые требования ЦБ РФ.

Сертификация и интеграция международных стандартов: адаптация ISO/IEC 27001 к российским требованиям, аудит соответствия, практика применения стандартов в российских организациях.

Содержание практических занятий

№ темы	Наименование темы, по которой предусмотрено практическое занятие	Формы и методы проведения
2.1.	Правовая база защиты информации в РФ	Выполнение практических заданий, обмен опытом
2.2.	Требования ФСТЭК и ФСБ России	Выполнение практических заданий, обмен опытом
2.3.	Персональные данные: права субъектов и обязанности операторов	Выполнение практических заданий, обмен опытом

2.4.	Международное регулирование и отраслевые стандарты	Выполнение практических заданий, обмен опытом
------	--	---

Рекомендуемый перечень практических заданий

Практические задания по Тема 2.1 «Правовая база защиты информации в РФ»

Задание 1.

Составьте классификатор нормативных правовых актов РФ в области защиты информации по уровням: Конституция РФ, федеральные законы (149-ФЗ, 152-ФЗ, 98-ФЗ, 187-ФЗ), подзаконные акты. Для каждого акта укажите дату принятия, сферу применения и ключевые положения. Оформите результат в виде таблицы.

Задание 2.

Определите категорию информации (общедоступная, ограниченного доступа, конфиденциальная) для десяти предложенных примеров документов. Обоснуйте каждую классификацию со ссылкой на конкретный нормативный акт.

Задание 3.

Разберите два кейса о нарушениях в области защиты информации: определите применимые статьи УК РФ или КоАП РФ, вид ответственности и возможные санкции. Подготовьте краткое заключение по каждому кейсу.

Практические задания по Тема 2.2 «Требования ФСТЭК и ФСБ России»

Задание 1.

Изучите приказ ФСТЭК России № 17 и определите требования к защите для информационной системы, обрабатывающей информацию ограниченного доступа. Определите класс защищённости и необходимые меры защиты. Оформите чек-лист соответствия.

Задание 2.

Рассчитайте уровень защищённости персональных данных для гипотетической организации (ИСПДн) по приказу ФСТЭК № 21. Опишите требуемые организационные и технические меры. Составьте краткий план приведения системы в соответствие.

Задание 3.

Изучите требования ФСБ России к криптографической защите информации (СКЗИ). Составьте перечень условий применения СКЗИ в организации и порядок получения лицензии. Подготовьте вывод о применимости требований к конкретному сценарию.

Практические задания по Тема 2.3 «Персональные данные: права субъектов и обязанности операторов»

Задание 1.

Составьте карту процессов обработки персональных данных для гипотетической организации: какие ПДн обрабатываются, с какой целью, на

каком правовом основании, кто является оператором и третьими лицами. Оформите в виде схемы.

Задание 2.

Разработайте образец согласия субъекта на обработку персональных данных в соответствии с 152-ФЗ. Проверьте его на соответствие требованиям закона (цели, перечень данных, срок действия, порядок отзыва).

Задание 3.

Разберите кейс об утечке персональных данных: определите действия оператора в первые часы и в последующие дни, применимые нормы 152-ФЗ, 270-ФЗ и 420-ФЗ, порядок уведомления Роскомнадзора и субъектов ПДн.

Практические задания по Тема 2.4 «Международное регулирование и отраслевые стандарты»

Задание 1.

Сравните требования 152-ФЗ и GDPR к обработке персональных данных: согласие, права субъектов, локализация, штрафы, порядок реагирования на инциденты. Оформите результаты в виде сравнительной таблицы.

Задание 2.

Изучите структуру стандарта ISO/IEC 27001 и составьте перечень основных разделов и мер контроля. Определите, какие из мер обязательны, а какие — рекомендательные. Подготовьте план внедрения СМИБ в небольшой организации.

Задание 3.

Разберите требования стандарта PCI DSS для организации, обрабатывающей платёжные карты: составьте чек-лист соответствия по 12 основным требованиям стандарта и определите уровни комплаенса.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с конспектами лекций, решения практических задач, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд библиотеки и Интернет-ресурсы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и учебные материалы, разработанные профессорско-преподавательским составом, конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей.

Преподаватель проводит офлайн консультацию слушателей для оценивания полноты и уровня самостоятельного освоения материала.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения и проводится в образовательной среде.

№ темы	Наименование темы	Формы и методы проведения
2.1.	Правовая база защиты информации в РФ	Изучение основной и дополнительной литературы по программе; выполнение практических заданий
2.2.	Требования ФСТЭК и ФСБ России	Изучение основной и дополнительной литературы по программе; выполнение практических заданий
2.3.	Персональные данные: права субъектов и обязанности операторов	Изучение основной и дополнительной литературы по программе; выполнение практических заданий
2.4.	Международное регулирование и отраслевые стандарты	Изучение основной и дополнительной литературы по программе; выполнение практических заданий

Рекомендуемый перечень вопросов для отработки в часы самостоятельной работы, подготовки к промежуточной аттестации

Тема 2.1. Правовая база защиты информации в РФ

1. Что такое информация и информационная безопасность в понимании 149-ФЗ?
2. Какова иерархия нормативных правовых актов в области защиты информации?
3. Какие категории информации по доступности выделяет законодательство?
4. Что такое конфиденциальная информация и как она защищается?
5. Что регулирует 187-ФЗ «О безопасности критической информационной инфраструктуры»?
6. Какие виды ответственности предусмотрены за нарушения в области защиты информации?
7. Какие статьи УК РФ касаются неправомерного доступа к информации?
8. Какова роль ФСТЭК России в области защиты информации?
9. Какова роль ФСБ России и Роскомнадзора?
10. Что такое государственная тайна и как она защищается?

Тема 2.2. Требования ФСТЭК и ФСБ России

1. Каковы основные функции ФСТЭК России в области технической защиты информации?
2. Что регулирует приказ ФСТЭК России № 17?
3. Что регулирует приказ ФСТЭК России № 21?
4. Что регулирует приказ ФСТЭК России № 239?
5. Что такое классы защищённости информационных систем и как они определяются?
6. Какова роль ФСБ России в области криптографической защиты информации?
7. Что такое СКЗИ и каковы требования к их использованию?
8. Что такое аттестация объектов информатизации и как она проводится?
9. Как определяются уровни защищённости персональных данных?
10. Какие документы необходимы для аттестации объекта информатизации?

Тема 2.3. Персональные данные: права субъектов и обязанности операторов

1. Что такое персональные данные и какие их категории выделяет 152-ФЗ?
2. Какие права имеет субъект персональных данных?
3. Какие обязанности возложены на оператора персональных данных?
4. Каков порядок получения согласия на обработку персональных данных?
5. Что такое локализация персональных данных на территории РФ?
6. Каков порядок уведомления Роскомнадзора об обработке ПДн?
7. Что такое трансграничная передача персональных данных и как она регулируется?
8. Какая ответственность предусмотрена за утечку персональных данных?
9. Что такое обезличивание персональных данных?
10. Каков порядок реагирования оператора на инцидент с персональными данными?

Тема 2.4. Международное регулирование и отраслевые стандарты

1. Что такое Будапештская конвенция о киберпреступности?
2. Каковы основные принципы GDPR?
3. В чём различия между 152-ФЗ и GDPR?
4. Что такое ISO/IEC 27001 и какова её структура?
5. Что такое NIST CSF и как она применяется?
6. Что такое PCI DSS и кому он обязателен?
7. Что такое ГОСТ Р 57580 и в каких случаях он применяется?
8. Какие требования ЦБ РФ действуют в области информационной безопасности?
9. Как международные стандарты интегрируются с российскими требованиями?

10. Что такое аудит соответствия стандартам информационной безопасности?

Перечень основной и дополнительной учебной литературы, необходимой для освоения модуля 2

Основная литература:

1. Баранова Е. К., Бабаш А. В. «Информационная безопасность и защита информации» — базовый учебник, охватывающий правовые и организационные аспекты.
2. Бабаш А. В., Мельников Ю. Н. «Правовое обеспечение информационной безопасности» — правовые основы защиты информации в РФ.
3. Хорев П. Б. «Правовая защита информации» — комментарии к нормативным актам, практические аспекты применения.
4. Кузнецов И. Н. «Информационная безопасность и защита информации» — учебное пособие по нормативно-правовому регулированию.
5. Соколова О. И., Бабаш А. В. «Информационные технологии и право» — обзор правового регулирования в цифровом обществе.
6. Мельников В. П. «Информационная безопасность» — учебник для вузов с акцентом на организационные и правовые меры.

Дополнительная литература:

1. 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. 152-ФЗ «О персональных данных».
3. 98-ФЗ «О коммерческой тайне».
4. 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».
5. Приказы ФСТЭК России № 17, № 21, № 239.
6. GDPR (Общий регламент ЕС по защите данных).
7. ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности».
8. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций».
9. PCI DSS v4.0 «Payment Card Industry Data Security Standard».

Интернет-ресурсы:

1. Официальный сайт ФСТЭК России (fstec.ru) — нормативные документы, методические рекомендации, реестры средств защиты.
2. Официальный сайт ФСБ России (fsb.ru) — требования к СКЗИ, лицензирование, методические документы.
3. Портал персональных данных Роскомнадзора (pd.rkn.gov.ru) — нормативные акты, реестр операторов, разъяснения.
4. Официальный интернет-портал правовой информации (pravo.gov.ru) — актуальные редакции законов и подзаконных актов.

5. Портал НКЦКИ (cve.fstec.ru) — база уязвимостей и рекомендации по безопасности.
6. Международная организация по стандартизации (iso.org) — тексты стандартов ISO/IEC серии 27000.
7. Официальный сайт PCI Security Standards Council (pcisecuritystandards.org) — документация PCI DSS.
8. Консультант Плюс и Гарант — системы правовой информации с комментариями нормативных актов.

Рабочая программа Модуля 3.

Модуль 3. Управление информационной безопасностью и оценка рисков

Учебно-тематический план модуля 3

Наименование разделов и тем	Трудоемкость, з.е.	Всего часов	Внеаудиторная работа			Самостоятельная работа, часов	Форма контроля
			всего	в т.ч. лекции	в т.ч. практические		
Модуль 3. Управление информационной безопасностью и оценка рисков							
Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001	0,25	10	3	1	2	7	зачет
Тема 3.2. Политика безопасности и организационно-распорядительная документация	0,25	10	3	1	2	7	диф. зачет методом тестирования
Тема 3.3. Оценка и управление рисками ИБ	0,25	10	3	1	2	7	зачет
Тема 3.4. Внутренний аудит и анализ защищенности	0,25	10	3	1	2	7	диф. зачет методом тестирования
Общая трудоемкость	1	40	12	4	8	28	

модуля 3							
----------	--	--	--	--	--	--	--

Содержание модуля 3

Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001

Понятие системы менеджмента информационной безопасности (СМИБ). Семейство стандартов ISO/IEC 27000: назначение и взаимосвязь документов.

Требования ISO/IEC 27001: контекст организации, лидерство и политика, планирование, поддержка и функционирование, оценка результативности, улучшение. Цикл PDCA применительно к СМИБ.

Область применения СМИБ, декларация о применимости (SoA), меры защиты по Приложению А, обоснование исключений.

Сертификация СМИБ: этапы, выбор органа по сертификации, поддержание сертификата, интегрированные системы менеджмента.

Тема 3.2. Политика безопасности и организационно-распорядительная документация

Политика информационной безопасности верхнего уровня: назначение, структура, требования к содержанию.

Иерархия документов по ИБ: политики, стандарты, процедуры, регламенты, инструкции; уровни детализации.

Порядок разработки, согласования, утверждения, введения в действие и пересмотра организационно-распорядительной документации (ОРД).

Матрица ролей и ответственности в области ИБ; доведение политики до персонала, ознакомление работников под подпись, контроль исполнения требований.

Тема 3.3. Оценка и управление рисками ИБ

Основные понятия управления рисками: актив, угроза, уязвимость, вероятность, последствия, уровень риска.

Методики оценки рисков: FRAP, OCTAVE, Методика определения актуальных угроз безопасности информации ФСТЭК России.

Идентификация и оценка активов, шкалы вероятности и ущерба, матрица рисков «вероятность – ущерб», ведение реестра рисков.

Стратегии обработки рисков: снижение, принятие, перенос, уклонение; план обработки рисков, остаточный риск, мониторинг и пересмотр.

Тема 3.4. Внутренний аудит и анализ защищённости

Внутренний аудит СМИБ по ISO/IEC 19011: принципы аудита, программа аудитов, план и этапы проведения.

Методы аудита: интервью, наблюдение за процессами, анализ документов и записей; типичные несоответствия и их классификация.

Анализ защищённости: сканирование уязвимостей, тестирование на проникновение, банк данных угроз ФСТЭК (БДУ), CIS Benchmarks.

Отчетность и метрики ИБ: показатели результативности СМИБ, отчет по итогам аудита, корректирующие мероприятия, анализ со стороны руководства.

Содержание практических занятий

№ темы	Наименование темы	Наименование практического занятия	Формы и методы проведения
3.1	Тема 3.1. Система менеджмента ИБ по	Разбор структуры ISO/IEC 27001;	Работа со стандартом в группах, кейс-анализ,

	ISO/IEC 27001	построение области применения СМИБ; составление фрагмента декларации о применимости	обсуждение результатов
3.2	Тема 3.2. Политика безопасности и организационно-распорядительная документация	Разработка проекта политики ИБ верхнего уровня; составление матрицы ролей и ответственности	Проектная работа в малых группах, взаимная экспертиза документов, мозговой штурм
3.3	Тема 3.3. Оценка и управление рисками ИБ	Инвентаризация и категорирование активов; оценка рисков по методике ФСТЭК; построение матрицы и реестра рисков	Практикум с рабочими таблицами, разбор кейса, работа в командах
3.4	Тема 3.4. Внутренний аудит и анализ защищённости	Подготовка чек-листа внутреннего аудита; разбор результатов сканирования уязвимостей; разработка отчета по аудиту	Деловая игра «Внутренний аудит», демонстрация сканера уязвимостей, разбор отчетов

Рекомендуемый перечень практических заданий

Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001

Задание 1. Определение области применения СМИБ

Действия: 1) выбрать организацию для учебного случая; 2) определить границы СМИБ и перечень охватываемых процессов; 3) составить перечень активов и заинтересованных сторон; 4) оформить обоснование области применения (1–2 страницы).

Задание 2. Составление декларации о применимости (SoA)

Действия: 1) изучить перечень мер Приложения А ISO/IEC 27001; 2) выбрать применимые меры защиты; 3) обосновать исключения; 4) оформить таблицу SoA с указанием статуса реализации мер.

Задание 3. Построение цикла PDCA для СМИБ

Действия: 1) распределить процессы организации по этапам Plan–Do–Check–Act; 2) указать примеры действий и документов на каждом этапе; 3) оформить схему цикла с комментариями.

Тема 3.2. Политика безопасности и организационно-распорядительная документация

Задание 4. Разработка проекта политики информационной безопасности

Действия: 1) изучить типовые структуры политики ИБ; 2) сформулировать цели, область действия, обязательства руководства и персонала; 3) оформить проект политики верхнего уровня (2–3 страницы).

Задание 5. Составление матрицы ролей и ответственности

Действия: 1) определить процессы ИБ (управление рисками, контроль доступа, реагирование на инциденты и др.); 2) распределить роли по модели RACI; 3) оформить матрицу ответственности.

Задание 6. Экспертиза организационно-распорядительного документа

Действия: 1) получить фрагмент типового регламента; 2) проверить соблюдение порядка согласования, утверждения и пересмотра; 3) составить перечень выявленных замечаний и предложить исправления.

Тема 3.3. Оценка и управление рисками ИБ

Задание 7. Инвентаризация и категорирование активов

Действия: 1) составить перечень информационных и технических активов учебной организации; 2) присвоить категории критичности; 3) назначить владельцев активов; 4) оформить таблицу активов.

Задание 8. Оценка рисков по методике ФСТЭК России

Действия: 1) изучить Методику определения актуальных угроз; 2) выбрать модель нарушителя; 3) определить актуальные угрозы; 4) рассчитать уровень риска и построить матрицу «вероятность – ущерб».

Задание 9. Составление реестра и плана обработки рисков

Действия: 1) внести оцененные риски в реестр; 2) выбрать стратегии обработки; 3) назначить меры, сроки и ответственных; 4) определить допустимый остаточный риск.

Тема 3.4. Внутренний аудит и анализ защищённости

Задание 10. Подготовка плана и чек-листа внутреннего аудита

Действия: 1) определить область и критерии аудита по ISO/IEC 19011; 2) составить план аудита; 3) разработать чек-лист проверочных вопросов по разделам СМИБ.

Задание 11. Анализ результатов сканирования уязвимостей

Действия: 1) изучить отчет сканера уязвимостей (учебный пример); 2) классифицировать находки по критичности; 3) сопоставить с записями в БДУ ФСТЭК; 4) подготовить рекомендации по устранению.

Задание 12. Разработка отчета по итогам внутреннего аудита

Действия: 1) систематизировать выявленные несоответствия; 2) сформулировать выводы о результативности СМИБ; 3) предложить корректирующие мероприятия со сроками и ответственными; 4) оформить отчет.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с конспектами лекций, решения практических задач, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд библиотеки и Интернет-ресурсы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и учебные материалы, разработанные профессорско-преподавательским составом, конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей. Преподаватель проводит офлайн консультацию слушателей для оценивания полноты и уровня самостоятельного освоения материала.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения и проводится в образовательной среде.

Наименование темы	Виды самостоятельной работы
Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001	Изучение текста ISO/IEC 27001 и конспектов лекций; составление глоссария терминов СМИБ; подготовка краткого конспекта по структуре стандарта; выполнение тестовых заданий
Тема 3.2. Политика безопасности и организационно-распорядительная документация	Работа с основной и дополнительной литературой; анализ примеров политик ИБ открытых организаций; подготовка проекта фрагмента политики; подготовка к практическому занятию
Тема 3.3. Оценка и управление рисками ИБ	Изучение Методики определения актуальных угроз ФСТЭК России; решение задач по оценке рисков; подготовка таблицы активов и реестра рисков к практическому занятию
Тема 3.4. Внутренний аудит и анализ защищённости	Изучение ISO/IEC 19011 и материалов по аудиту ИБ; подготовка к деловой игре «Внутренний аудит»; выполнение тестовых заданий; подготовка к промежуточной аттестации

Перечень вопросов для подготовки к зачету (дифференцированному зачету)

Тема 3.1. Система менеджмента ИБ по ISO/IEC 27001

1. Понятие и назначение системы менеджмента информационной безопасности.
2. Семейство стандартов ISO/IEC 27000: состав и назначение документов.
3. Цикл PDCA и его применение к управлению ИБ.
4. Требования разделов 4–10 ISO/IEC 27001: краткая характеристика.
5. Контекст организации и заинтересованные стороны при построении СМИБ.
6. Роль руководства и политика ИБ в СМИБ.
7. Область применения СМИБ: как и зачем она определяется.
8. Декларация о применимости (SoA): назначение и порядок составления.
9. Меры защиты по Приложению А: группы и принципы выбора.
10. Порядок сертификации СМИБ и поддержания сертификата.

Тема 3.2. Политика безопасности и организационно-распорядительная документация

1. Понятие политики информационной безопасности верхнего уровня.
2. Иерархия документов по ИБ: политики, стандарты, процедуры, инструкции.
3. Требования к содержанию политики ИБ.
4. Порядок разработки и согласования документов по ИБ.
5. Утверждение, введение в действие и пересмотр ОРД.
6. Матрица ролей и ответственности в области ИБ.
7. Доведение требований политики до персонала: способы и документирование.
8. Контроль исполнения требований организационно-распорядительных документов.
9. Типичные ошибки при разработке внутренних документов по ИБ.
10. Связь политики ИБ с требованиями ISO/IEC 27001 и законодательства РФ.

Тема 3.3. Оценка и управление рисками ИБ

1. Понятия «актив», «угроза», «уязвимость», «риск»: определения и взаимосвязь.
2. Этапы процесса управления рисками ИБ.

3. Методика определения актуальных угроз ФСТЭК России: назначение и применение.
4. Методики FRAP и OCTAVE: область применения и отличия.
5. Идентификация и категорирование активов.
6. Шкалы вероятности и ущерба, матрица рисков «вероятность – ущерб».
7. Реестр рисков: структура и порядок ведения.
8. Стратегии обработки рисков: сравнительная характеристика.
9. Остаточный риск: понятие и порядок принятия.
10. Мониторинг и пересмотр рисков в процессе деятельности организации.

Тема 3.4. Внутренний аудит и анализ защищённости

1. Назначение и принципы внутреннего аудита СМИБ.
2. Стандарт ISO/IEC 19011: область применения и требования.
3. Программа и план аудита: порядок разработки.
4. Методы аудита: интервью, наблюдение, анализ документов.
5. Классификация несоответствий по результатам аудита.
6. Отчет по итогам аудита: структура и требования.
7. Корректирующие мероприятия: порядок реализации и контроля.
8. Сканирование уязвимостей как метод анализа защищённости.
9. Тестирование на проникновение: назначение и отличия от сканирования.
10. Банк данных угроз ФСТЭК (БДУ) и его использование при анализе защищённости.

Литература

Основная литература:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ФОРУМ: ИНФРА-М.
2. Баранова Е.К., Бабид А.В. Информационная безопасность и защита информации: учебное пособие. – М.: РИОР: ИНФРА-М.
3. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие. – М.: ФОРУМ: ИНФРА-М.

Дополнительная литература:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
2. ISO/IEC 27005. Information security risk management.
3. ISO/IEC 19011:2018. Guidelines for auditing management systems.
4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций.
5. Методика определения актуальных угроз безопасности информации. – М.: ФСТЭК России, 2021.

Интернет-ресурсы:

1. ФСТЭК России: официальный сайт – www.fstec.ru.
2. Банк данных угроз безопасности информации ФСТЭК России (БДУ) – bdu.fstec.ru.
3. ISO – International Organization for Standardization – www.iso.org.
4. Официальный интернет-портал правовой информации – pravo.gov.ru.
5. Роскомнадзор: персональные данные – pd.rkn.gov.ru.

РАБОЧАЯ ПРОГРАММА
Модуля 4. «Криптографические методы защиты информации»

Учебно-тематический план модуля 4

Наименование разделов и тем	Трудоемкость, з.е. / час	Внеаудиторная работа, всего	Лекции	Практические занятия	Самостоятельная работа	Форма контроля
Модуль 4. Криптографические методы защиты информации	1 / 40	12	4	8	28	
Тема 4.1. Основы криптографии и симметричное шифрование	0,25 / 10	3	1	2	7	зачет
Тема 4.2. Асимметричная криптография и электронная подпись	0,25 / 10	3	1	2	7	диф. зачет методом тестирования
Тема 4.3. Хэширование, целостность и аутентификация данных	0,25 / 10	3	1	2	7	зачет
Тема 4.4. Управление ключами и инфраструктура открытых ключей	0,25 / 10	3	1	2	7	диф. зачет методом тестирования
Итого по модулю 4	1 з.е. / 40 часов	12	4	8	28	

Содержание модуля 4. Криптографические методы защиты информации

Тема 4.1. Основы криптографии и симметричное шифрование

Предмет и история криптографии. Принцип Керкгоффса. Криптография и криптоанализ. Симметричные шифры: потоковые и блочные. Длина ключа и его стойкость.

Режимы работы блочных шифров: ECB, CBC, CFB, OFB, CTR, GCM. Уязвимости режима ECB.

Отечественный стандарт блочного шифрования ГОСТ Р 34.12-2015 («Магма», «Кузнечик»), режимы по ГОСТ Р 34.13-2015.

Зарубежные алгоритмы: DES, 3DES, AES. Набивка данных (padding).

Тема 4.2. Асимметричная криптография и электронная подпись

Математические основы: простые числа, модульная арифметика, теорема Эйлера. Задача факторизации и дискретного логарифмирования.

Алгоритм RSA: генерация ключей, шифрование и расшифрование. Алгоритм Эль-Гамала.

Протокол Диффи–Хеллмана и атака «человек посередине».

Криптография на эллиптических кривых. ГОСТ Р 34.10-2012.

Электронная подпись по 63-ФЗ: простая, усиленная неквалифицированная и квалифицированная подпись. Операторы ЭП.

Практическое применение: TLS, PGP/GnuPG, S/MIME.

Тема 4.3. Хэширование, целостность и аутентификация данных

Свойства криптографических хэш-функций. Коллизии и атака «дней рождения».

ГОСТ Р 34.11-2012 («Стрибог»), семейство SHA-2, SHA-3 (Кескак).

Хранение паролей: соль, замедленные функции (bcrypt, scrypt, Argon2).

Имитовставка и коды аутентификации сообщений: CBC-MAC, CMAC, HMAC, ГОСТ Р 34.13-2015.

Контроль целостности файлов и данных. Практические схемы аутентификации.

Тема 4.4. Управление ключами и инфраструктура открытых ключей

Жизненный цикл криптографических ключей: генерация, распределение, хранение, ротация, уничтожение.

Криптосистемы с открытым ключом на практике: PGP, GnuPG, веб доверия.

Инфраструктура открытых ключей (PKI): центры сертификации, сертификаты X.509, цепочки доверия, отзыв сертификатов (CRL, OCSP).

Российская PKI: головной удостоверяющий центр, корневые УЦ, электронная подпись на Госуслугах.

Требования ФСБ России к средствам криптографической защиты информации (СКЗИ) и их сертификация.

Аппаратные модули безопасности (HSM). Протокол TLS и его настройки. Постквантовая криптография.

Содержание практических занятий

Наименование темы	Содержание практических занятий	Формы и методы проведения
Тема 4.1. Основы криптографии и симметричное шифрование	Классификация шифров, режимы работы блочных шифров, стандарты ГОСТ Р 34.12-2015 и AES. Лабораторная работа: шифрование файлов средствами OpenSSL.	Лабораторная работа, разбор кейсов
Тема 4.2. Асимметричная криптография и электронная подпись	Асимметричные алгоритмы RSA и Диффи–Хеллмана, ГОСТ Р 34.10-2012. Разбор видов электронной подписи по 63-ФЗ.	Деловая игра «Оформление электронной подписи», кейс-анализ
Тема 4.3. Хэширование, целостность и аутентификация данных	Хэш-функции ГОСТ Р 34.11-2012 и SHA-2, хранение паролей, имитовставки и HMAC. Лабораторная работа: контрольные суммы и	Лабораторная работа, решение задач

	проверка целостности.	
Тема 4.4. Управление ключами и инфраструктура открытых ключей	Жизненный цикл ключей, PKI, сертификаты X.509, российская PKI и требования ФСБ к СКЗИ. Проектирование схемы PKI организации.	Проектная работа, разбор кейсов

Рекомендуемый перечень практических заданий

Тема 4.1. Основы криптографии и симметричное шифрование

Задание 1. Составить сравнительную таблицу симметричных алгоритмов (AES, «Магма», «Кузнечик», 3DES): длина ключа, размер блока, режимы работы, области применения.

Задание 2. Выполнить шифрование файла средствами OpenSSL: генерация ключей, шифрование в режимах CBC и GCM, расшифрование и проверка результата.

Задание 3. Продемонстрировать уязвимость режима ECB: зашифровать растровое изображение в режимах ECB и CBC, сравнить и объяснить результат.

Тема 4.2. Асимметричная криптография и электронная подпись

Задание 4. Выполнить расчёт RSA на малых числах: выбрать p и q , вычислить n , функцию Эйлера, открытую и закрытую экспоненты, зашифровать сообщение вручную и проверить программно.

Задание 5. Смоделировать протокол Диффи–Хеллмана в паре с другим слушателем, продемонстрировать атаку «человек посередине» и способ её предотвращения.

Задание 6. Изучить структуру квалифицированного сертификата электронной подписи: найти серию, срок действия, владельца, издателя и путь доверия.

Тема 4.3. Хэширование, целостность и аутентификация данных

Задание 7. Вычислить контрольные суммы файлов с помощью ГОСТ Р 34.11-2012 и SHA-256, сравнить результаты и скорость вычисления.

Задание 8. Продемонстрировать влияние соли на стойкость хранения паролей: подобрать хэш без соли и с солью, оценить применимость Argon2.

Задание 9. Построить HMAC для сообщения по ГОСТ Р 34.13-2015, проверить целостность при модификации сообщения.

Тема 4.4. Управление ключами и инфраструктура открытых ключей

Задание 10. Развёрнуть локальный центр сертификации (OpenSSL CA или XCA): выпустить корневой сертификат, пользовательские сертификаты и выполнить их отзыв.

Задание 11. Проанализировать TLS-сертификат произвольного сайта: цепочка доверия, срок действия, применённые алгоритмы, статус проверки отзыва.

Задание 12. Разработать проект регламента управления криптографическими ключами организации: классификация ключей, сроки ротации, порядок хранения и уничтожения.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей в процессе освоения программы (модуля, дисциплины) состоит из изучения основной и дополнительной литературы по программе, ознакомления с конспектами лекций, решения практических задач, выполнения тестовых заданий, подготовки к итоговой аттестации. Для подготовки и выполнения заданий для самостоятельной работы слушатели используют книжный фонд библиотеки и Интернет-ресурсы.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса.

Слушателям предоставляются: программа курса, список рекомендованной литературы и учебные материалы, разработанные профессорско-преподавательским составом, конспекты лекций, контрольные и тестовые задания для практических занятий.

После самостоятельного изучения материала проводятся консультации для дополнительного пояснения вопросов, вызвавших затруднения у слушателей. Преподаватель проводит онлайн консультацию слушателей для оценивания полноты и уровня самостоятельного освоения материала.

Индивидуальная консультационная работа преподавателей со слушателями осуществляется весь период обучения и проводится в образовательной среде.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 4.1. Основы криптографии и симметричное шифрование	Изучение основной и дополнительной литературы по теме, конспектов лекций. Выполнение практических заданий 1–3. Подготовка к зачету.	7
Тема 4.2. Асимметричная криптография и электронная подпись	Изучение литературы и нормативных документов по теме, конспектов лекций. Выполнение практических заданий 4–6. Подготовка к диф. зачету методом тестирования.	7
Тема 4.3. Хэширование, целостность и аутентификация данных	Изучение литературы по теме, конспектов лекций. Выполнение практических заданий 7–9. Подготовка к зачету.	7
Тема 4.4. Управление ключами и инфраструктура открытых ключей	Изучение литературы по теме, конспектов лекций. Выполнение практических заданий 10–12. Подготовка к диф. зачету методом тестирования.	7
Итого		28

Перечень вопросов для самостоятельной подготовки

Тема 4.1. Основы криптографии и симметричное шифрование

1. Что изучает криптография и чем она отличается от криптоанализа?
2. Сформулируйте принцип Керкгоффса и объясните его значение.
3. Чем потоковые шифры отличаются от блочных?
4. Как длина ключа влияет на стойкость алгоритма шифрования?
5. Опишите режим CBC и его преимущества перед режимом ECB.
6. Почему режим ECB считается небезопасным? Приведите пример.
7. Опишите алгоритм «Кузнечик» стандарта ГОСТ Р 34.12-2015.
8. Опишите алгоритм «Магма» и его историю происхождения.
9. Как устроен алгоритм AES? Какие преобразования применяются в раунде?
10. Что такое набивка данных (padding) и какие схемы набивки применяются?

Тема 4.2. Асимметричная криптография и электронная подпись

1. В чём принципиальное отличие асимметричной криптографии от симметричной?
2. Опишите этапы генерации ключей в алгоритме RSA.
3. Какая математическая задача обеспечивает стойкость RSA?
4. Опишите протокол Диффи–Хеллмана и его назначение.
5. В чём состоит атака «человек посередине» и как её предотвратить?
6. Какие преимущества даёт криптография на эллиптических кривых?
7. Опишите алгоритм электронной подписи ГОСТ Р 34.10-2012.
8. Какие виды электронной подписи установлены 63-ФЗ и чем они различаются?

9. Какие функции выполняет оператор электронной подписи?
10. Где на практике применяется асимметричная криптография (TLS, PGP, S/MIME)?

Тема 4.3. Хэширование, целостность и аутентификация данных

1. Какими свойствами должна обладать криптографическая хэш-функция?
2. Что такое коллизия хэш-функции и в чём состоит атака «дней рождения»?
3. Опишите алгоритм «Стрибог» (ГОСТ Р 34.11-2012).
4. Чем SHA-3 отличается от SHA-2?
5. Почему нельзя хранить пароли в виде простого хэша?
6. Что такое соль и как она повышает стойкость хранения паролей?
7. Опишите работу функций bcrypt, scrypt, Argon2.
8. Что такое имитовставка и для чего она применяется?
9. Как устроен HMAC и какие ключи в нём используются?
10. Каким образом проверяется целостность загруженных файлов и программного обеспечения?

Тема 4.4. Управление ключами и инфраструктура открытых ключей

1. Перечислите этапы жизненного цикла криптографических ключей.
2. Какие требования предъявляются к генерации ключей?
3. Опишите модель веб доверия PGP и её отличия от PKI.
4. Какие функции выполняет центр сертификации в PKI?
5. Какова структура сертификата X.509 и какие поля в нём обязательны?
6. Как происходит отзыв сертификата: CRL и OCSP?
7. Опишите российскую национальную PKI и роль головного удостоверяющего центра.
8. Какие требования ФСБ России предъявляются к СКЗИ и их сертификации?
9. Для чего применяются аппаратные модули безопасности (HSM)?
10. Что такое постквантовая криптография и какие направления в ней развиваются?

Литература и интернет-ресурсы

Основная литература:

Панасенко С.П. Алгоритмы шифрования. Специальный справочник. — СПб.: БХВ-Петербург.
Шаньгин В.Ф. Информационная безопасность и защита информации. — М.: ДМК Пресс.
Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия–Телеком.

Нормативные правовые акты и стандарты:

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.
ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи.
Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении требований к средствам электронной подписи».

Интернет-ресурсы:

Официальный сайт ФСБ России — fsb.ru.

Официальный сайт Минцифры России — digital.gov.ru.

Официальный интернет-портал правовой информации — pravo.gov.ru.

Рабочая программа

Модуль 5. Безопасность сетевой инфраструктуры

Учебно-тематический план модуля 5

Наименование модулей, тем	Всего часов	Внеаудиторная работа, часов		Самостоятельная работа, часов	Форма контроля
		лекции	практические занятия		
Модуль 5. Безопасность сетевой инфраструктуры	40	4 8		28	зачет
Тема 5.1. Архитектура защищённых сетей и сегментирование	10	3	2	7	диф. зачет методом тестирования
Тема 5.2. Межсетевое экранирование и контроль трафика	10	3	2	7	диф. зачет методом тестирования
Тема 5.3. Обнаружение вторжений и анализ сетевого трафика	10	3	2	7	диф. зачет методом тестирования
Тема 5.4. VPN-технологии и защищённый удалённый доступ	10	3	2	7	диф. зачет методом тестирования
Итого по модулю 5:	40	4	8	28	диф. зачет методом тестирования

Общая трудоемкость модуля 5 — 1 з.е. (40 часов).

Содержание модуля 5

Тема 5.1. Архитектура защищённых сетей и сегментирование

- Концепция зон безопасности: внутренняя сеть, периметр, DMZ, гостевые и производственные сегменты. Принципы сегментирования: наименьшие привилегии, минимально необходимая связность, доверенные зоны.
- Схемы сетевой архитектуры: плоская сеть и её риски, иерархическая модель (ядро — распределение — доступ), сегментация по VLAN и маршрутизацией, NAT и его роль на периметре.
- Микросегментация и Zero Trust: принцип «никому не доверяй, проверяй всё», программно-определяемые сети, политики east-west трафика, типовые ошибки проектирования сегментации.

Тема 5.2. Межсетевое экранирование и контроль трафика

- Назначение и классы межсетевых экранов: пакетные фильтры, шлюзы прикладного уровня, межсетевые экраны нового поколения (NGFW).
- Правила фильтрации: принцип «запрещено всё, что не разрешено», порядок применения правил, объектные группы, трансляция адресов (SNAT, DNAT), публикация сервисов через DMZ.
- Инспекция протоколов: контроль HTTP/HTTPS, DNS, FTP; противодействие обходу фильтрации через туннели и нестандартные порты. Системы предотвращения вторжений (IPS) как модуль МЭ.

Тема 5.3. Обнаружение вторжений и анализ сетевого трафика

- Системы обнаружения вторжений: сигнатурные и аномальные IDS/IPS, сетевые и хостовые, схемы размещения (за МЭ, внутри сегментов).
- Методы анализа трафика: зеркалирование портов (SPAN), сетевые TAP, сниферы Wireshark и tcpdump, разбор структуры сетевых пакетов, выявление сканирования, аномалий и туннелирования.
- Корреляция событий: системы SIEM, нормализация и агрегирование логов, база данных уязвимостей БДУ ФСТЭК России, стандарт CIS Benchmarks для настройки сетевого оборудования.

Тема 5.4. VPN-технологии и защищённый удалённый доступ

- Протоколы VPN: IPsec (IKE, ESP, AH), TLS-VPN (OpenVPN), WireGuard. Схемы site-to-site и remote access, выбор схемы под задачу организации.
- Аутентификация и авторизация удалённого доступа: сертификаты, RADIUS и LDAP, многофакторная аутентификация (MFA), сетевой контроль доступа (NAC).
- Эксплуатация VPN: управление правами и сессиями, аудит подключений, требования к СКЗИ при использовании VPN на территории РФ (приказы ФСБ России), типовые ошибки конфигурации.

Содержание практических занятий модуля 5

Наименование темы	Формы и методы проведения практических занятий
Тема 5.1. Архитектура защищённых сетей и сегментирование	Проектирование схемы сегментированной сети: разбор кейса, выбор зон и правил связности, защита проекта.
Тема 5.2. Межсетевое экранирование и контроль трафика	Лабораторная работа: настройка правил межсетевого экрана в виртуальной среде; разбор типовых ошибок конфигурации.
Тема 5.3. Обнаружение вторжений и анализ	Лабораторная работа: анализ дампа трафика в

сетевого трафика	Wireshark, выявление признаков сканирования; кейс-разбор сигнатур IDS.
Тема 5.4. VPN-технологии и защищённый удалённый доступ	Лабораторная работа: развёртывание VPN-туннеля и настройка двухфакторной аутентификации; деловая игра «Аудит удалённого доступа подрядчика».

Рекомендуемый перечень практических заданий модуля 5

Тема 5.1. Архитектура защищённых сетей и сегментирование

Задание 1. Построить схему сегментированной сети организации: выделить зоны (периметр, DMZ, внутренние сегменты, сегмент АСУ), обозначить точки контроля трафика. Оформить схему и обосновать выбор границ сегментов.

Задание 2. Составить матрицу допустимых потоков между сегментами: определить, какие службы и в каком направлении доступны каждой зоне, указать протоколы и порты. Проверить матрицу на соответствие принципу наименьших привилегий.

Задание 3. Проанализировать типовые ошибки сегментации на заданной архитектуре: найти «мостики» между зонами, необоснованные широковебательные домены и избыточные маршруты. Предложить варианты устранения.

Тема 5.2. Межсетевое экранирование и контроль трафика

Задание 4. Составить базовый набор правил межсетевого экрана для организации с DMZ: разрешить публикацию web-сервера, запретить прямой доступ из интернета во внутреннюю сеть, настроить трансляцию адресов. Обосновать каждое правило.

Задание 5. Провести аудит готового набора правил МЭ: выявить избыточные, конфликтующие и чрезмерно широкие правила, предложить сокращённый вариант набора.

Задание 6. Разобрать сценарий обхода фильтрации (туннелирование через разрешённый протокол, нестандартный порт). Предложить контрмеры: сигнатуры IPS, ограничения прикладного уровня, контроль DNS.

Тема 5.3. Обнаружение вторжений и анализ сетевого трафика

Задание 7. Провести анализ дампа трафика в Wireshark: найти признаки сетевого сканирования, определить цели и тип сканера. Составить краткий отчёт по наблюдаемой активности.

Задание 8. Настроить в виртуальной среде систему обнаружения вторжений: подключить набор правил, сгенерировать тестовую активность, проверить срабатывания и разобрать ложные срабатывания.

Задание 9. Составить перечень событий сетевого оборудования для передачи в SIEM: определить источники логов, ключевые события и пороги оповещения. Оформить таблицу «событие — источник — действие».

Тема 5.4. VPN-технологии и защищённый удалённый доступ

Задание 10. Развернуть VPN-туннель site-to-site между двумя виртуальными сетями: настроить параметры шифрования и аутентификации, проверить связность и целостность трафика.

Задание 11. Настроить remote access VPN с многофакторной аутентификацией: выпустить сертификаты, подключить второй фактор, оформить регламент выдачи и отзыва доступа сотрудицам.

Задание 12. Провести аудит удалённого доступа подрядчика: проверить права, сроки действия учётных записей, журнал подключений; составить отчёт с перечнем замечаний и рекомендаций.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей организуется в соответствии с учебно-тематическим планом модуля и включает изучение рекомендуемой литературы, нормативных правовых актов и стандартов, подготовку конспектов и выполнение практических заданий.

Слушатели обеспечиваются необходимыми учебно-методическими материалами. По итогам каждого занятия предусмотрены консультации преподавателей, в ходе которых слушатели могут получить разъяснения по изучаемым вопросам.

Контроль усвоения материала осуществляется в форме проверки выполненных заданий и итогового тестирования по модулю.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 5.1. Архитектура защищённых сетей и сегментирование	Изучение принципов сегментирования и архитектуры Zero Trust; проработка схемы сети организации; выполнение заданий 1–3; подготовка к защите схемы. Форма контроля — обсуждение на занятии.	7
Тема 5.2. Межсетевое экранирование и контроль трафика	Изучение классов межсетевых экранов и принципов составления правил; работа с виртуальной средой; выполнение заданий 4–6. Форма контроля — проверка набора правил МЭ.	7
Тема 5.3. Обнаружение вторжений и анализ сетевого трафика	Практика анализа трафика в Wireshark; изучение сигнатур и структуры логов; выполнение заданий 7–9. Форма контроля — отчёт по анализу дампа.	7
Тема 5.4. VPN-технологии и защищённый удалённый доступ	Изучение протоколов IPsec, TLS-VPN, WireGuard и требований к СКЗИ; выполнение заданий 10–12; подготовка к итоговому тестированию. Форма контроля — диф. зачет методом тестирования.	7
Итого:		28

Перечень вопросов для самоконтроля и итогового контроля по модулю 5

Тема 5.1. Архитектура защищённых сетей и сегментирование

1. Что такое зона безопасности и какие зоны принято выделять в корпоративной сети?
2. Назовите принципы сегментирования сети. Почему плоская сеть считается небезопасной?
3. Какие задачи решает DMZ и какие сервисы в ней обычно размещают?
4. Чем отличаются сегментация по VLAN и маршрутизация между сегментами?
5. Что такое микросегментация и чем она отличается от классической сегментации?
6. В чём суть концепции Zero Trust и какие требования она предъявляет к сетевой архитектуре?
7. Какую роль играет NAT на сетевом периметре и какие ограничения он создаёт?

8. Какие типовые ошибки допускают при проектировании сегментированной сети?
9. Как определяется связность между сегментами и как её документируют?
10. Какие нормативные требования предъявляются к архитектуре защищённых сетей?

Тема 5.2. Межсетевое экранирование и контроль трафика

1. Назовите классы межсетевых экранов и их отличия по принципу работы.
2. В чём различия между пакетным фильтром и шлюзом прикладного уровня?
3. Какие возможности добавляют межсетевые экраны нового поколения (NGFW)?
4. Сформулируйте правило «запрещено всё, что не разрешено» и его значение.
5. От чего зависит порядок применения правил фильтрации и как избежать конфликтов?
6. Для чего используются SNAT и DNAT и в чём их различие?
7. Как правильно организовать публикацию внутреннего сервиса через DMZ?
8. Какие угрозы создаёт туннелирование трафика и как МЭ противодействует ему?
9. Чем отличается IPS от IDS и где каждый из них размещается?
10. Какие требования к межсетевым экранам установлены нормативными актами ФСТЭК России?

Тема 5.3. Обнаружение вторжений и анализ сетевого трафика

1. В чём различие сигнатурного и аномального методов обнаружения вторжений?
2. Чем сетевые IDS/IPS отличаются от хостовых?
3. Какие схемы размещения систем обнаружения вторжений применяются и как их выбрать?
4. Что такое зеркалирование портов (SPAN) и сетевой TAP, в чём их различия?
5. Какие возможности Wireshark используются при анализе сетевого трафика?
6. По каким признакам в трафике выявляют сетевое сканирование?
7. Что такое туннелирование трафика и как его обнаружить средствами анализа?
8. Какие функции выполняет SIEM и какие события в неё передаются?
9. Для чего предназначена база данных уязвимостей БДУ ФСТЭК России?
10. Что представляют собой рекомендации CIS Benchmarks для сетевого оборудования?

Тема 5.4. VPN-технологии и защищённый удалённый доступ

1. Какие компоненты входят в протокол IPsec и какие функции выполняют ESP и AH?
2. Как работает протокол IKE и для чего он используется в IPsec?
3. В чём преимущества и ограничения TLS-VPN (OpenVPN) по сравнению с IPsec?
4. Как устроен протокол WireGuard и почему он считается производительным?
5. Чем отличается схема site-to-site от remote access VPN?
6. Какие методы аутентификации применяются при организации удалённого доступа?
7. Для чего нужна многофакторная аутентификация и какие факторы она объединяет?
8. Что такое NAC и какие проверки он выполняет при подключении устройства?
9. Какие требования к СКЗИ предъявляются при использовании VPN на территории РФ?
10. Как организуется аудит VPN-подключений и какие события фиксируются?

Рекомендуемая литература по модулю 5

Основная литература:

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. — М.: ФОРУМ: ИНФРА-М.
3. Партыка Т. Л., Попов И. И. Информационная безопасность. — М.: ФОРУМ: ИНФРА-М.

Дополнительная литература:

1. ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, кибербезопасность и защита информации. Системы менеджмента информационной безопасности. Требования.
2. Приказ ФСТЭК России от 20.06.2011 № 240 (и действующие редакции требований по защите информации в государственных ИС).
3. Национальный стандарт РФ ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций.

Интернет-ресурсы:

1. Официальный сайт ФСТЭК России — www.fstec.ru.
2. База данных уязвимостей БДУ ФСТЭК России — bdu.fstec.ru.
3. Официальный интернет-портал правовой информации — www.pravo.gov.ru.
4. Официальный сайт ФСБ России — www.fsb.ru.

МОДУЛЬ 6**«Безопасность информационных систем и защита информации»****Учебно-тематический план****Учебно-тематический план модуля 6**

Наименование темы	Всего часов				
	в том числе	лекции	практические занятия	самостоятель ная работа слушателей	Форма контроля
Модуль 6. Безопасность веб- приложений и защищённая разработка	10	1	2	7	зачет
Тема 6.1. Типовые уязвимости веб- приложений	10	1	2	7	зачет
Тема 6.2. Методы защищённой разработки ПО	10	1	2	7	диф. зачет методом тестирования
Тема 6.3. Аутентификация, сессии и управление доступом в веб	10	1	2	7	зачет
Тема 6.4. Практикум: поиск и устранение уязвимостей	10	1	2	7	диф. зачет методом тестирования
Итого по модулю 6	40	4	8	28	

Общая трудоемкость модуля 6: 1 з.е. / 40 часов	
---	--

Содержание модуля

Тема 6.1. Типовые уязвимости веб-приложений

Статистика и таксономия уязвимостей; OWASP Top 10 и OWASP API Security Top 10; инъекции: SQL, NoSQL, командные; XSS: отражённая, хранимая, DOM; CSRF; SSRF; IDOR и ошибки контроля доступа; небезопасная загрузка файлов; десериализация; логические уязвимости; CVE, CWE, CVSS как языки описания уязвимостей.

Тема 6.2. Методы защищённой разработки ПО

Подход Shift-Left и Security by Design; моделирование угроз приложений (STRIDE); безопасный жизненный цикл разработки (SDL, NIST SSDF); статический и динамический анализ: SAST, DAST, IAST, SCA; управление зависимостями и SBOM; безопасная обработка ввода, параметризованные запросы, экранирование вывода; защита секретов в коде и CI/CD; безопасная конфигурация окружения.

Тема 6.3. Аутентификация, сессии и управление доступом в веб

Модели аутентификации; пароли: хранение (bcrypt, Argon2), политика сложности, сброс пароля; управление сессиями: cookies, токены, JWT и их типовые ошибки; протоколы делегирования: OAuth 2.0 и OpenID Connect; многофакторная аутентификация; модели контроля доступа: RBAC, ABAC; защита браузера: атрибуты cookies (HttpOnly, Secure, SameSite), CSP, HSTS; обход аутентификации и захват сессий.

Тема 6.4. Практикум: поиск и устранение уязвимостей

Методология тестирования веб-приложений (OWASP WSTG); инструменты: Burp Suite, OWASP ZAP, SQLMap, анализаторы кода; воспроизведение уязвимостей на тестовом стенде; классификация и приоритизация по CVSS 3.1; составление отчёта об уязвимости и рекомендаций по устранению; проверка исправлений и регрессионное тестирование; взаимодействие с командой разработки.

Содержание практических занятий

Наименование темы	Формы проведения практических занятий
Тема 6.1. Типовые уязвимости веб-приложений	Разбор реальных инцидентов по типовым уязвимостям OWASP Top 10; лабораторная работа по воспроизведению инъекций и XSS на учебном стенде; кейс-анализ ошибок контроля доступа (IDOR) в демо-приложении.
Тема 6.2. Методы защищённой разработки ПО	Лабораторная работа со статическим анализатором кода (SAST) и проверкой зависимостей (SCA); моделирование угроз приложения по методике STRIDE в мини-группах; разбор правил безопасного CI/CD-пайплайна.
Тема 6.3. Аутентификация, сессии и управление доступом в веб	Лабораторная работа по настройке аутентификации и сессий в учебном веб-

	приложении; анализ JWT-токенов и типовых ошибок их использования; кейс-анализ ошибок OAuth 2.0 и реализации контроля доступа.
Тема 6.4. Практикум: поиск и устранение уязвимостей	Командный квест по поиску уязвимостей в тестовом приложении с Burp Suite и OWASP ZAP; составление отчётов об уязвимостях с оценкой по CVSS; проверка исправлений и регрессионное тестирование.

Рекомендуемый перечень практических заданий

Тема 6.1. Типовые уязвимости веб-приложений

Задание 1. Классифицировать уязвимости в описаниях инцидентов по категориям OWASP Top 10 и указать для каждой соответствующий CWE, обосновав выбор.

Задание 2. Воспроизвести SQL-инъекцию и отражённую XSS в учебном приложении на тестовом стенде, описать механизмы атак и возможные последствия.

Задание 3. Найти уязвимость типа IDOR в демо-приложении: проанализировать запросы к API, продемонстрировать доступ к чужим данным и предложить исправление.

Тема 6.2. Методы защищённой разработки ПО

Задание 4. Провести статический анализ исходного кода учебного приложения (SAST), отсортировать найденные замечания по критичности и подготовить список исправлений.

Задание 5. Выполнить проверку сторонних зависимостей проекта (SCA), выявить компоненты с известными CVE и предложить план их обновления с учётом SBOM.

Задание 6. Построить модель угроз небольшого веб-приложения по методике STRIDE и составить перечень контрмер для выявленных рисков.

Тема 6.3. Аутентификация, сессии и управление доступом в веб

Задание 7. Настроить в учебном приложении корректное управление сессиями: атрибуты cookies (HttpOnly, Secure, SameSite), тайм-ауты и защиту от фиксации сессии.

Задание 8. Проанализировать выданные JWT-токены: проверить подпись, срок действия и типовые ошибки реализации; продемонстрировать последствия небезопасной конфигурации.

Задание 9. Спроектировать схему контроля доступа (RBAC) для учебного портала: определить роли, права и проверить отсутствие горизонтальных и вертикальных обходов.

Тема 6.4. Практикум: поиск и устранение уязвимостей

Задание 10. Провести сканирование тестового веб-приложения (Burp Suite, OWASP ZAP), отделить подтверждённые уязвимости от ложных срабатываний.

Задание 11. Оценить найденные уязвимости по CVSS 3.1 и составить отчёт об уязвимостях с рекомендациями по устранению и приоритетами.

Задание 12. Для уязвимости, устранённой разработчиком, составить план регрессионного тестирования и проверить корректность исправления повторным тестом.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей организуется в форме изучения учебных и нормативно-технических материалов, выполнения практических заданий и подготовки к контрольным мероприятиям. Общий объём самостоятельной работы по модулю составляет 28 часов (по 7 часов на каждую тему).

Результаты самостоятельной работы проверяются в рамках текущего и итогового контроля по модулю.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 6.1. Типовые уязвимости веб-приложений	Изучение учебных материалов по теме; проработка OWASP Top 10; выполнение практических заданий 1–3; подготовка к текущему контролю (зачет).	7
Тема 6.2. Методы защищённой разработки ПО	Изучение учебных материалов по теме; проработка требований NIST SSDF; выполнение практических заданий 4–6; подготовка к текущему контролю (диф. зачет методом тестирования).	7
Тема 6.3. Аутентификация, сессии и управление доступом в веб	Изучение учебных материалов по теме; проработка документации по OAuth 2.0 и OpenID Connect; выполнение практических заданий 7–9; подготовка к текущему контролю (зачет).	7
Тема 6.4. Практикум: поиск и устранение уязвимостей	Изучение учебных материалов по теме; проработка методики OWASP WSTG; выполнение практических заданий 10–12; подготовка к итоговому контролю (диф. зачет методом тестирования).	7
Итого по модулю 6		28

Контрольные вопросы по модулю

Тема 6.1. Типовые уязвимости веб-приложений

1. Почему SQL-инъекция остаётся одной из самых распространённых уязвимостей и как её предотвращать?
2. В чём различие отражённой, хранимой и DOM-моделей XSS?
3. Какие механизмы защиты от CSRF существуют и как они работают?
4. Чем SSRF опасен для внутренней инфраструктуры организации?
5. Что такое IDOR и как правильно реализовать контроль доступа к объектам?
6. Какие риски связаны с небезопасной загрузкой файлов на сервер?
7. Как классифицируются уязвимости в стандартах CWE и оцениваются по CVSS?

8. Какие логические уязвимости сложнее всего выявить автоматизированными средствами и почему?
9. Как связаны OWASP API Security Top 10 и OWASP Top 10?
10. Как корректно проверять уязвимость, не нанося ущерба рабочей системе?

Тема 6.2. Методы защищённой разработки ПО

1. Что такое подход Shift-Left и какие преимущества он даёт?
2. В чём состоит методика моделирования угроз STRIDE?
3. Какие требования предъявляет NIST SSDF к процессу разработки?
4. Чем различаются SAST, DAST, IAST и SCA? В каких случаях применим каждый метод?
5. Что такое SBOM и зачем он нужен организации?
6. Какие правила безопасной обработки пользовательского ввода обязательны для разработчика?
7. Почему параметризованные запросы устраняют SQL-инъекции?
8. Как защитить секреты (ключи, пароли) в репозитории и CI/CD-пайплайне?
9. Что такое безопасные по умолчанию (secure by default) настройки фреймворков?
10. Как организовать процесс исправления уязвимостей в команде разработки?

Тема 6.3. Аутентификация, сессии и управление доступом в веб

1. Какие требования предъявляются к безопасному хранению паролей?
2. Чем различаются bcrypt и Argon2 и какой алгоритм предпочтителен?
3. Из каких частей состоит JWT и какие ошибки чаще всего допускают при его использовании?
4. Чем аутентификация отличается от авторизации?
5. Как устроен протокол OAuth 2.0 и какие типы разрешений (grant types) в нём существуют?
6. Что такое OpenID Connect и как он связан с OAuth 2.0?
7. Какие методы многофакторной аутентификации применяются в веб-приложениях?
8. В чём различие моделей контроля доступа RBAC и ABAC?
9. Какие атрибуты cookies влияют на безопасность сессии и как именно?
10. Какие меры защиты дают заголовки CSP и HSTS?

Тема 6.4. Практикум: поиск и устранение уязвимостей

1. Из каких этапов состоит методика тестирования веб-приложений OWASP WSTG?
2. Какие возможности предоставляет Burp Suite для ручного тестирования?
3. Какие ограничения имеет автоматическое сканирование OWASP ZAP и как учитывать ложные срабатывания?
4. Как рассчитывается базовая оценка уязвимости по CVSS 3.1?
5. Какие разделы должен содержать корректный отчёт об уязвимости?

6. Как приоритизировать устранение уязвимостей при ограниченных ресурсах?
7. Что такое регрессионное тестирование и зачем оно проводится после исправления?
8. Как безопасно проверить уязвимость на работающей системе?
9. Как выстроить взаимодействие специалистов ИБ с командой разработки при устранении уязвимостей?
10. Какие метрики уязвимостей полезно отслеживать на уровне организации?

Основная литература:

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. — М.: ФОРУМ: ИНФРА-М.

Партыка Т. Л., Попов И. И. Информационная безопасность. — М.: ФОРУМ: ИНФРА-М.

ГОСТ Р ИСО/МЭК 27001-2021. Системы менеджмента информационной безопасности. Требования.

Дополнительная литература:

OWASP Testing Guide (WSTG). — OWASP Foundation.

OWASP Application Security Verification Standard (ASVS). — OWASP Foundation.

RFC 6749. The OAuth 2.0 Authorization Framework. — IETF.

RFC 7519. JSON Web Token (JWT). — IETF.

NIST SP 800-53. Security and Privacy Controls for Information Systems.

Интернет-ресурсы:

Официальный сайт OWASP Foundation — owasp.org

База данных уязвимостей и слабых сторон — cwe.mitre.org, nvd.nist.gov

ФСТЭК России — fstec.ru

Официальный интернет-портал правовой информации — pravo.gov.ru

Рабочая программа профессионального модуля

Модуль 7. Защита данных: персональные данные, облака и резервирование

Учебно-тематический план

Наименование темы	Всего часов	Лекции	Практические занятия	Самостоятельная работа	Форма контроля
Модуль 7. Защита данных: персональные данные, облака и резервирование	40	4	8	28	зачет
Тема 7.1. Управление доступом и разграничение прав	10	1	2	7	зачет
Тема 7.2. Шифрование данных в покое и при передаче	10	1	2	7	диф. зачет методом тестирования
Тема 7.3. Резервное копирование и восстановление систем	10	1	2	7	зачет
Тема 7.4. Безопасность облачных сервисов и ПДн	10	1	2	7	диф. зачет методом тестирования
Итого по модулю 7	40	4	8	28	—

Содержание модуля

Тема 7.1. Управление доступом и разграничение прав

Понятие и модели управления доступом; дискреционное и мандатное разграничение прав. Ролевая (RBAC) и атрибутная (ABAC) модели доступа, их сравнение и области применения. Принцип наименьших привилегий и управление жизненным циклом учётных записей. Привилегированный доступ (PAM), сервисные учётные записи, аудит и регулярный пересмотр прав доступа.

Тема 7.2. Шифрование данных в покое и при передаче

Шифрование данных в покое: шифрование дисков и томов (LUKS, BitLocker), прозрачное шифрование СУБД и шифрование на уровне приложений. Управление ключами шифрования: KMS, HSM, хранение и ротация ключей. Шифрование при передаче: протокол TLS 1.3, взаимная аутентификация (mTLS). Отечественные стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.10-2012, требования 152-ФЗ и постановления Правительства РФ № 313 к СКЗИ.

Тема 7.3. Резервное копирование и восстановление систем

Роль резервного копирования в обеспечении непрерывности деятельности. Стратегии копирования: полное, инкрементальное, дифференциальное; правило 3-2-1. Показатели RPO и RTO и их влияние на архитектуру резервирования. Тестирование восстановления, защита копий от программ-шифровальщиков, план непрерывности и восстановления после аварий (BCP/DRP).

Тема 7.4. Безопасность облачных сервисов и ПДн

Модель разделения ответственности в облаке; модели IaaS, PaaS, SaaS. Персональные данные: категории и требования 152-ФЗ. Уровни защищённости ПДн (постановление Правительства РФ № 1119) и меры по приказу ФСТЭК России № 21. Локализация данных, критерии оценки облачного провайдера, безопасность объектных хранилищ (S3) и инфраструктуры как кода (IaC).

Содержание практических занятий

Наименование темы	Содержание практических занятий	Количество часов
Тема 7.1. Управление доступом и разграничение прав	Лабораторная работа «Проектирование ролевой модели доступа (RBAC)»;	2

	кейс-анализ избыточных прав и сервисных учётных записей.	
Тема 7.2. Шифрование данных в покое и при передаче	Лабораторная работа «Шифрование раздела диска и данных СУБД»; лабораторная работа «Настройка защищённого канала TLS».	2
Тема 7.3. Резервное копирование и восстановление систем	Лабораторная работа «Резервное копирование и восстановление данных»; разбор кейса восстановления после атаки шифровальщика.	2
Тема 7.4. Безопасность облачных сервисов и ПДн	Кейс-анализ выбора облачного провайдера для обработки ПДн; лабораторная работа «Аудит доступа к объектному хранилищу».	2
Итого		8

Перечень практических заданий

Тема 7.1. Управление доступом и разграничение прав

Задание 1. Проектирование ролевой модели доступа (RBAC) для подразделения: выделение ролей, построение матрицы прав, оформление результатов.

Задание 2. Аудит учётных записей и прав в тестовой системе: выявление избыточных привилегий, неактивных и сервисных учётных записей, подготовка предложений по устранению.

Задание 3. Настройка принципа наименьших привилегий в тестовой системе; разбор кейса компрометации сервисной учётной записи.

Тема 7.2. Шифрование данных в покое и при передаче

Задание 4. Практикум по шифрованию раздела диска (LUKS или BitLocker): включение шифрования, проверка доступности данных и поведения при утере ключа.

Задание 5. Настройка защищённого канала TLS: установка сертификатов, включение TLS 1.3, проверка конфигурации и наборов шифров.

Задание 6. Сравнительный анализ сценариев шифрования данных «в покое» и «при передаче»; выбор СКЗИ с учётом требований 152-ФЗ и постановления № 313.

Тема 7.3. Резервное копирование и восстановление систем

Задание 7. Разработка плана резервного копирования для учебной информационной системы с расчётом RPO и RTO.

Задание 8. Выполнение полного, инкрементального и дифференциального копирования; восстановление файлов из резервных копий и проверка целостности.

Задание 9. Разбор кейса восстановления после инцидента с программой-шифровальщиком: оценка роли неизменяемых копий и порядка восстановления.

Тема 7.4. Безопасность облачных сервисов и ПДн

Задание 10. Оценка облачного сервиса на соответствие требованиям 152-ФЗ: категория обрабатываемых ПДн, уровень защищённости, локализация данных.

Задание 11. Аудит настроек доступа к объектному хранилищу (S3): поиск публичных бакетов, анализ прав доступа и включённого шифрования.

Задание 12. Разработка чек-листа безопасности облачного внедрения с распределением ответственности между провайдером и заказчиком.

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей включает изучение лекционного материала и дополнительной литературы по темам модуля, выполнение практических заданий и подготовку отчётов по ним, проработку контрольных вопросов, а также подготовку к итоговому контролю по модулю.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 7.1. Управление доступом и разграничение прав	Изучение теоретического материала по управлению доступом; проектирование ролевой модели доступа для подразделения; подготовка отчёта по заданиям 1–3; проработка контрольных вопросов темы. Форма контроля: зачет.	7
Тема 7.2. Шифрование данных в покое и при передаче	Изучение стандартов шифрования и нормативных требований к СКЗИ; настройка шифрования данных в тестовой среде; подготовка отчёта по заданиям 4–6; проработка контрольных вопросов темы. Форма контроля: диф. зачет методом тестирования.	7
Тема 7.3. Резервное копирование и восстановление систем	Изучение стратегий резервного копирования; разработка плана резервного копирования и восстановления; подготовка отчёта по заданиям 7–9; проработка контрольных вопросов темы. Форма контроля: зачет.	7
Тема 7.4. Безопасность облачных сервисов и ПДн	Изучение требований 152-ФЗ к обработке ПДн; анализ облачного сервиса по чек-листу; подготовка отчёта по заданиям 10–12; проработка контрольных вопросов темы. Форма контроля: диф. зачет методом тестирования.	7
Итого по модулю 7		28

Перечень контрольных вопросов

Тема 7.1. Управление доступом и разграничение прав

1. Понятие управления доступом и его место в системе защиты информации.
2. Дискреционная модель разграничения доступа: сущность, преимущества и ограничения.
3. Мандатная модель доступа и многоуровневая безопасность.
4. Ролевая модель доступа (RBAC): роли, матрица прав, порядок внедрения.

5. Атрибутная модель доступа (ABAC) и сферы её применения.
6. Принцип наименьших привилегий и способы его реализации.
7. Жизненный цикл учётных записей: создание, изменение, блокирование, удаление.
8. Управление привилегированным доступом (PAM): задачи и средства.
9. Сервисные (технологические) учётные записи: риски и правила обращения.
10. Аудит прав доступа и регулярный пересмотр полномочий.

Тема 7.2. Шифрование данных в покое и при передаче

1. Понятие шифрования данных в покое и при передаче.
2. Шифрование дисков и томов: LUKS, BitLocker, сценарии применения.
3. Шифрование на уровне СУБД и приложений: прозрачное шифрование, шифрование полей.
4. Управление ключами шифрования: KMS, HSM, хранение и ротация ключей.
5. Протокол TLS и его роль в защите данных при передаче; TLS 1.3.
6. Взаимная аутентификация TLS (mTLS) и сценарии её применения.
7. Российские стандарты шифрования: ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012.
8. Нормативные требования к применению СКЗИ: 152-ФЗ и постановление Правительства РФ № 313.
9. Сравнительный анализ отечественных и зарубежных алгоритмов шифрования.
10. Типовые ошибки при внедрении шифрования данных и способы их предотвращения.

Тема 7.3. Резервное копирование и восстановление систем

1. Назначение резервного копирования и его место в обеспечении непрерывности.
2. Стратегии резервного копирования: полное, инкрементальное, дифференциальное.
3. Правило 3-2-1 и схемы хранения резервных копий.
4. Показатели RPO и RTO: определение, расчёт, влияние на архитектуру резервирования.
5. Виды носителей и хранилищ для резервных копий, облачное резервирование.
6. Тестирование восстановления: методика, регулярность, документирование результатов.
7. Защита резервных копий: шифрование, разграничение доступа, неизменяемые копии.
8. Угроза программ-шифровальщиков для резервных копий и меры защиты.
9. План непрерывности деятельности и план восстановления после аварий (BCP/DRP).
10. Типовые ошибки при организации резервного копирования.

Тема 7.4. Безопасность облачных сервисов и ПДн

1. Модель разделения ответственности между провайдером и заказчиком в облаке.
2. Модели облачных сервисов IaaS, PaaS, SaaS и распределение мер защиты.
3. Персональные данные: категории, цели обработки, 152-ФЗ.
4. Уровни защищённости ПДн и требования постановления Правительства РФ № 1119.
5. Требования приказа ФСТЭК России № 21 к системам обработки ПДн.
6. Локализация персональных данных при использовании облачных сервисов.
7. Критерии выбора облачного провайдера для обработки ПДн.

8. Безопасность объектных хранилищ (S3): разграничение доступа, шифрование.
9. Аудит и оценка безопасности облачного провайдера.
10. Безопасность инфраструктуры как кода (IaC) при работе с облаками.

Литература

Основная литература

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. — М.: ИНФРА-М.

Партыка Т.Л., Попов И.И. Информационная безопасность. — М.: ФОРУМ.

Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия–Телеком.

Дополнительная литература и нормативные документы

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 01.04.2021 № 313 «Об утверждении требований к шифровальным (криптографическим) средствам, предназначенным для шифрования персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

ГОСТ Р ИСО/МЭК 27001–2021. Системы менеджмента информационной безопасности. Требования.

ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

Интернет-ресурсы

Официальный сайт ФСТЭК России — fstec.ru.

Портал операторов персональных данных — pd.rkn.gov.ru.

Официальный сайт ФСБ России — fsb.ru.

Официальный интернет-портал правовой информации — pravo.gov.ru.

Cloud Security Alliance — cloudsecurityalliance.org.

Рабочая программа Модуля 8.

Модуль 8. Управление инцидентами информационной безопасности

Учебно-тематический план

Наименование темы	Всего часов	В том числе			Форма контроля
		лекции	практические	самостоятельная работа	
Тема 8.1. Организация процесса реагирования на инциденты	10	1	2	7	зачет
Тема 8.2. Инструменты мониторинга и SIEM	10	1	2	7	диф. зачет методом тестирования
Тема 8.3. Основы цифровой криминалистики	10	1	2	7	зачет
Тема 8.4. Человеческий фактор и обучение персонала	10	1	2	7	диф. зачет методом тестирования
Модуль 8. Управление инцидентами информационной безопасности	1 з.е. / 40	4	8	28	зачет / диф. зачет методом тестирования

Содержание модуля

Тема 8.1. Организация процесса реагирования на инциденты

Жизненный цикл реагирования на инциденты (NIST SP 800-61): подготовка, обнаружение и анализ, локализация, ликвидация, восстановление, извлечение уроков. Планы реагирования (IRP): структура, роли, матрица ответственности и процедуры эскалации. Классификация и приоритизация инцидентов: критичность, влияние на бизнес, метрики MTTD, MTTR, MTTA. Взаимодействие с командой реагирования (CSIRT), юридические аспекты и уведомление регуляторов. Разработка сценариев реагирования (playbook). Tabletop-упражнения и командные тренировки.

Тема 8.2. Инструменты мониторинга и SIEM

Централизованный сбор журналов: источники, агенты, форматы, нормализация. Архитектура и компоненты SIEM: корреляция событий, правила, дашборды и оповещения. Правила корреляции: настройка, борьба с ложными срабатываниями, приоритезация алертов. Автоматизация реагирования (SOAR): сценарии, интеграции. EDR/XDR: контроль конечных точек, изоляция хостов. Проактивный поиск угроз (Threat Hunting) по индикаторам компрометации (IoC), работа с тактиками и техниками MITRE ATT&CK. Мониторинг сетевого трафика и интеграция с системами обнаружения вторжений.

Тема 8.3. Основы цифровой криминалистики

Принципы цифровой криминалистики: неизменность доказательств, цепочка хранения улик (chain of custody), стандарты сбора данных. Снимки дисков и оперативной памяти, образы, хеширование и контроль целостности. Инструменты: Autopsy, FTK Imager, Volatility. Анализ артефактов операционных систем Windows и Linux: журнал событий, файлы реестра, задачи, сетевые подключения. Хронология инцидента (timeline), восстановление сценария атаки. Составление криминалистического отчёта. Антифорензика и её преодоление. Правовые основы работы с цифровыми уликами.

Тема 8.4. Человеческий фактор и обучение персонала

Социальная инженерия как вектор атак: фишинг, вишинг, бейтинг, предтекстинг. Программа Security Awareness: цели, содержание, аудитории, регулярность. Правила работы с паролями, почтой, мобильными устройствами и BYOD. Учебные фишинговые кампании: организация, метрики, обратная связь. Формирование культуры безопасности в организации: роль руководства, каналы коммуникации. Оценка эффективности обучения: тесты, симуляции, поведение персонала. Работа с инсайдерскими угрозами.

Содержание практических занятий

Наименование темы	Наименование практического занятия	Форма проведения
Тема 8.1. Организация процесса реагирования на инциденты	ПЗ 1. Разработка плана реагирования на инциденты (IRP) и матрицы ролей	Разбор кейса, проектирование документа
Тема 8.1. Организация процесса реагирования на инциденты	ПЗ 2. Классификация и приоритизация инцидентов	Работа с кейсами, разбор примеров
Тема 8.1. Организация процесса реагирования на инциденты	ПЗ 3. Tabletop-упражнение по сценарию инцидента	Командная тренировка, разбор результатов
Тема 8.2. Инструменты мониторинга и SIEM	ПЗ 4. Развертывание и настройка SIEM, сбор журналов	Лабораторная работа
Тема 8.2. Инструменты мониторинга и SIEM	ПЗ 5. Написание правил корреляции и разбор ложных срабатываний	Лабораторная работа
Тема 8.2. Инструменты мониторинга и SIEM	ПЗ 6. Проактивный поиск угроз по IoC и MITRE ATT&CK	Лабораторная работа
Тема 8.3. Основы цифровой криминалистики	ПЗ 7. Создание снимков диска и памяти, контроль целостности	Лабораторная работа
Тема 8.3. Основы цифровой криминалистики	ПЗ 8. Анализ артефактов в Autopsy и Volatility	Лабораторная работа
Тема 8.3. Основы цифровой криминалистики	ПЗ 9. Восстановление хронологии инцидента	Практикум, защита отчёта
Тема 8.4. Человеческий фактор и обучение персонала	ПЗ 10. Разработка программы обучения персонала	Проектирование, обсуждение
Тема 8.4. Человеческий фактор и обучение персонала	ПЗ 11. Учебная фишинговая кампания и разбор метрик	Лабораторная работа
Тема 8.4. Человеческий фактор и обучение персонала	ПЗ 12. Кейс: поведение персонала при инциденте	Ролевая игра, разбор

Перечень практических заданий для самостоятельной работы

Тема 8.1. Организация процесса реагирования на инциденты

Задание 1. Разработать план реагирования на инциденты (IRP) для организации среднего размера с ролями, порядком эскалации и контактами.

Задание 2. Составить матрицу классификации инцидентов: категории, критичность, приоритеты, сроки реакции.

Задание 3. Провести tabletop-упражнение по сценарию утечки данных и оформить извлечённые уроки.

Тема 8.2. Инструменты мониторинга и SIEM

Задание 4. Составить перечень источников журналов для организации и обосновать состав собираемых событий.

Задание 5. Написать пять правил корреляции для SIEM: обнаружение подбора пароля, аномальных входов, изменений в критичных каталогах.

Задание 6. Провести поиск угроз по предоставленным индикаторам компрометации и сопоставить действия с MITRE ATT&CK.

Тема 8.3. Основы цифровой криминалистики

Задание 7. Создать снимок диска и оперативной памяти тестовой системы, зафиксировать хеши и заполнить chain of custody.

Задание 8. Провести анализ образа в Autopsy: найти артефакты входа в систему и запуска программ.

Задание 9. Восстановить хронологию инцидента по предоставленному образу и составить краткий криминалистический отчет.

Тема 8.4. Человеческий фактор и обучение персонала

Задание 10. Разработать программу Security Awareness на год: темы, аудитории, форматы и расписание.

Задание 11. Спланировать учебную фишинговую кампанию: сценарий письма, метрики успеха, порядок обратной связи.

Задание 12. Составить правила работы персонала с паролями, почтой и мобильными устройствами (BYOD).

Содержание самостоятельной работы слушателей

Самостоятельная работа слушателей организуется в соответствии с рабочей программой и включает изучение рекомендованной литературы, выполнение практических заданий и подготовку к контрольным мероприятиям. Содержание и объем самостоятельной работы по темам модуля приведены в таблице.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 8.1. Организация процесса реагирования на инциденты	Изучение литературы по теме, выполнение заданий 1–3, подготовка к контрольному мероприятию (зачет).	7
Тема 8.2. Инструменты мониторинга и SIEM	Изучение литературы по теме, выполнение заданий 4–6, подготовка к контрольному мероприятию (диф. зачет методом тестирования).	7
Тема 8.3. Основы цифровой криминалистики	Изучение литературы по теме, выполнение заданий 7–9, подготовка к контрольному мероприятию (зачет).	7
Тема 8.4. Человеческий фактор и обучение персонала	Изучение литературы по теме, выполнение заданий 10–12, подготовка к контрольному мероприятию (диф. зачет методом тестирования).	7
Модуль 8. Управление инцидентами информационной безопасности	Итого по модулю 8	28

Перечень вопросов для самоконтроля

Тема 8.1. Организация процесса реагирования на инциденты

- Назовите этапы жизненного цикла реагирования на инциденты по NIST SP 800-61.
- Что такое план реагирования (IRP) и какие разделы он включает?
- Как распределяются роли и ответственность в инцидентной команде?
- Опишите процедуру эскалации инцидента.
- Какие критерии используются для классификации инцидентов?
- Как инциденты приоритизируются по критичности и влиянию на бизнес?
- Что такое метрики MTTD, MTTR, MTTA и как они применяются?
- Какова роль CSIRT и порядок взаимодействия с ним?
- Какие юридические обязанности возникают при инцидентах с персональными данными?
- Что такое playbook и tabletop-упражнение?

Тема 8.2. Инструменты мониторинга и SIEM

- Какие источники журналов собираются в централизованной системе мониторинга?
- Опишите типовую архитектуру SIEM и её компоненты.
- Как устроены правила корреляции событий?
- Как снизить количество ложных срабатываний?
- Что такое SOAR и какие сценарии автоматизации применяются?
- Какие возможности дают EDR и XDR на конечных точках?
- Что такое Threat Hunting и какие данные для него нужны?
- Что такое индикаторы компрометации (IoC)?
- Как используется матрица MITRE ATT&CK при анализе угроз?
- Как строится приоритезация оповещений в системе мониторинга?

Тема 8.3. Основы цифровой криминалистики

- Какие принципы обеспечивают неизменность цифровых доказательств?
- Что такое chain of custody и как он оформляется?
- Как снимаются образы дисков и памяти и чем они фиксируются?
- Какие возможности дают Autopsy, FTK Imager и Volatility?
- Какие артефакты Windows используются при расследовании?
- Какие артефакты Linux используются при расследовании?
- Как строится хронология инцидента (timeline)?
- Какова структура криминалистического отчёта?
- Что такое антифорензика и как она выявляется?
- Каковы правовые основы работы с цифровыми уликами?

Тема 8.4. Человеческий фактор и обучение персонала

- Почему человеческий фактор остаётся одним из главных векторов атак?
- Какие виды атак социальной инженерии существуют?
- Как устроена программа Security Awareness?
- Какие темы включают в обучение персонала по безопасности?
- Какие правила устанавливаются для паролей и почты?
- Что такое BYOD и какие риски он создаёт?
- Как проводятся учебные фишинговые кампании и какие метрики собираются?
- Какова роль руководства в культуре безопасности?
- Как оценивается эффективность обучения персонала?
- Какие признаки указывают на инсайдерскую угрозу?

Литература

Основная:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. — М.: ФОРУМ: ИНФРА-М.
2. Партыка Т. Л., Попов И. И. Информационная безопасность. — М.: ФОРУМ: ИНФРА-М.
3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Дополнительная:

4. NIST SP 800-61. Computer Security Incident Handling Guide.
5. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response.
6. MITRE ATT&CK. Matrix of adversary tactics and techniques. — attack.mitre.org
7. OWASP Security Awareness. — owasp.org

Интернет-ресурсы:

8. ФСТЭК России. — fstec.ru
9. Банк данных угроз безопасности информации ФСТЭК России. — bdu.fstec.ru
10. Национальный центр защиты информации ФСБ России. — fsb.ru
11. Официальный интернет-портал правовой информации. — pravo.gov.ru

Рабочая программа Модуля 9.

Модуль 9. Современные технологии в обеспечении информационной безопасности Учебно-тематический план

Наименование темы	Всего часов	В том числе:			Форма контроля
		Лекции	Практические занятия	Самостоятельная работа	
Тема 9.1. Искусственный интеллект и машинное обучение в ИБ	10	1	2	7	зачет
Тема 9.2. Блокчейн-технологии и безопасность распределённых систем	10	1	2	7	диф. зачет методом тестирования
Тема 9.3. Квантовая криптография и постквантовые алгоритмы	10	1	2	7	зачет
Тема 9.4. Автоматизация процессов ИБ и итоговая	10	1	2	7	диф. зачет методом тестирования

подготовка проекта					
Итого по модулю 9: 1 з.е. / 40 часов					

Содержание модуля

Модуль 9. Современные технологии в обеспечении информационной безопасности посвящён современным технологиям защиты информации: применению искусственного интеллекта и машинного обучения, безопасности блокчейн-систем и распределённых реестров, квантовой криптографии и постквантовым алгоритмам, а также автоматизации процессов ИБ. Завершается модуль итоговой подготовкой проекта слушателя.

Тема 9.1. Искусственный интеллект и машинное обучение в ИБ

- Обзор методов машинного обучения для ИБ: обучение с учителем и без учителя, обнаружение аномалий.
- Применение ML: выявление вредоносного ПО, фишинга и сетевых аномалий; поведенческая аналитика (UEBA).
- Качество данных и проблема ложных срабатываний в системах обнаружения.
- Атаки на модели: отравление данных, состязательные примеры, извлечение модели.
- Генеративный ИИ: возможности для защиты и риски (фишинг, дипфейки, prompt injection).
- Этические и правовые аспекты применения ИИ в ИБ.

Тема 9.2. Блокчейн-технологии и безопасность распределённых систем

- Основы блокчейн-технологий: распределённый реестр, механизмы консенсуса (PoW, PoS, BFT).
- Криптографические примитивы блокчейна: хэш-функции, подписи, Merkle-деревья.
- Смарт-контракты: типовые уязвимости (повторный вход, переполнение, ошибки контроля доступа).
- Аудит смарт-контрактов, классификация слабостей (SWC Registry), формальная верификация.
- Безопасность DeFi: атаки на мосты, оракулы и протоколы ликвидности.
- Блокчейн в корпоративных информационных системах: применение и ограничения.

Тема 9.3. Квантовая криптография и постквантовые алгоритмы

- Угроза квантовых вычислений для классической криптографии: алгоритмы Шора и Гровера.
- Атака «harvest now, decrypt later» и долгосрочная защита данных.
- Основы квантовой криптографии: протокол BB84, квантовое распределение ключей (QKD).
- Постквантовые алгоритмы NIST: ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+).
- Гибридные схемы шифрования и подписи, крипто-agility.
- Практика миграции: инвентаризация СКЗИ, планы перехода; отечественные разработки.

Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта

- Автоматизация процессов ИБ: SOAR, playbooks, автоматизация реагирования на инциденты.
- DevSecOps: встраивание безопасности в CI/CD, SAST и DAST в пайплайнах.
- Инфраструктура как код (IaC): Ansible, Terraform, аудит конфигураций.
- Автоматизация управления уязвимостями и патч-менеджмента.
- Метрики эффективности ИБ и отчётность для руководства.

– Итоговая подготовка проекта: разработка политики безопасности и архитектуры защиты ИС, защита проекта.

Содержание практических занятий

№ п/п	Тема	Наименование и содержание занятия	Форма проведения
1	Тема 9.1. Искусственный интеллект и машинное обучение в ИБ	Построение модели обнаружения аномалий в журналах аудита (обучение с учителем и без учителя)	Лабораторная работа
2	Тема 9.1. Искусственный интеллект и машинное обучение в ИБ	Анализ атак на модели машинного обучения: состязательные примеры и отравление данных	Разбор кейса
3	Тема 9.1. Искусственный интеллект и машинное обучение в ИБ	Оценка рисков применения генеративного ИИ в организации и разработка политики его использования	Практикум
4	Тема 9.2. Блокчейн-технологии и безопасность распределённых систем	Разбор уязвимости повторного входа (reentrancy) в смарт-контракте	Разбор кейса
5	Тема 9.2. Блокчейн-технологии и безопасность распределённых систем	Аудит смарт-контракта по чек-листу SWC Registry	Лабораторная работа
6	Тема 9.2. Блокчейн-технологии и безопасность распределённых систем	Анализ инцидента с DeFi-платформой или блокчейн-мостом и формулирование выводов	Разбор кейса
7	Тема 9.3. Квантовая криптография и постквантовые алгоритмы	Инвентаризация СКЗИ и оценка готовности организации к миграции на постквантовые алгоритмы	Практикум
8	Тема 9.3. Квантовая криптография и постквантовые алгоритмы	Сравнение постквантовых алгоритмов NIST по длине ключей и производительности	Лабораторная работа
9	Тема 9.3. Квантовая криптография и постквантовые алгоритмы	Проектирование гибридной схемы шифрования для защищённого канала связи	Практикум
10	Тема 9.4.	Автоматизация	Лабораторная работа

	Автоматизация процессов ИБ и итоговая подготовка проекта	разбора типового инцидента: разработка playbook для SOAR	
11	Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта	Аудит IaC-шаблона и настройка проверок безопасности в CI/CD	Лабораторная работа
12	Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта	Презентация и защита итогового проекта слушателя	Защита проекта

Перечень практических заданий

Тема 9.1. Искусственный интеллект и машинное обучение в ИБ

Задание 1. Построить и настроить модель обнаружения аномалий в журналах аудита; оценить долю ложных срабатываний и подобрать порог классификации.

Задание 2. Разобрать демонстрацию состязательной атаки на классификатор и атаки отравления обучающих данных; предложить меры защиты модели.

Задание 3. Составить политику безопасного применения генеративного ИИ в организации: допустимые сценарии, запреты, контроль утечек данных.

Тема 9.2. Блокчейн-технологии и безопасность распределённых систем

Задание 4. Проанализировать код смарт-контракта с уязвимостью повторного входа; описать сценарий атаки и исправленный вариант.

Задание 5. Провести аудит смарт-контракта по чек-листу SWC Registry; оформить перечень выявленных слабостей с рекомендациями.

Задание 6. Разобрать реальный инцидент с DeFi-платформой или мостом; построить схему атаки и предложить меры её предотвращения.

Тема 9.3. Квантовая криптография и постквантовые алгоритмы

Задание 7. Выполнить инвентаризацию СКЗИ организации и оценить готовность к миграции на постквантовые алгоритмы; составить план перехода.

Задание 8. Сравнить постквантовые алгоритмы NIST (ML-KEM, ML-DSA, SLH-DSA) по длине ключей, подписей и производительности; свести результаты в таблицу.

Задание 9. Спроектировать гибридную схему шифрования защищённого канала связи: сочетание классического и постквантового алгоритмов.

Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта

Задание 10. Разработать playbook для SOAR по автоматизации разбора типового инцидента; описать шаги, условия эскалации и метрики.

Задание 11. Выполнить аудит IaC-шаблона инфраструктуры; настроить проверки безопасности (SAST, IaC-сканирование) в CI/CD-пайплайне.

Задание 12. Подготовить итоговый проект: политику безопасности и архитектуру защиты ИС; провести презентацию и защиту проекта.

Содержание самостоятельной работы слушателей

Содержание самостоятельной работы слушателей определяется темами модуля и включает: изучение теоретического материала по темам модуля; выполнение практических заданий; подготовку к контрольным мероприятиям (зачету, дифференцированному зачету методом тестирования). На самостоятельную работу отводится 28 часов.

Наименование темы	Содержание самостоятельной работы	Количество часов
Тема 9.1. Искусственный интеллект и машинное обучение в ИБ	Изучение теоретического материала по теме; выполнение практических заданий 1–3; подготовка к зачету.	7
Тема 9.2. Блокчейн-технологии и безопасность распределённых систем	Изучение теоретического материала по теме; выполнение практических заданий 4–6; подготовка к дифференцированному зачету методом тестирования.	7
Тема 9.3. Квантовая криптография и постквантовые алгоритмы	Изучение теоретического материала по теме; выполнение практических заданий 7–9; подготовка к зачету.	7
Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта	Изучение теоретического материала по теме; выполнение практических заданий 10–12; подготовка итогового проекта и его защита.	7
Итого по модулю 9 — 28		

Контрольные вопросы

Тема 9.1. Искусственный интеллект и машинное обучение в ИБ

1. Какие методы машинного обучения применяются для обнаружения аномалий в сетевом трафике?
2. В чём различие между обучением с учителем и без учителя применительно к задачам ИБ?
3. Как работает поведенческая аналитика UEBA и какие источники данных она использует?
4. Почему ложные срабатывания считаются главной проблемой ML-систем обнаружения?
5. Что такое состязательные примеры и как они применяются против моделей машинного обучения?
6. Что такое отравление обучающих данных и как снизить этот риск?
7. Какие риски несёт применение генеративного ИИ злоумышленниками?
8. Что такое prompt injection и как уменьшить связанные с ним риски?
9. С помощью каких метрик оценивают качество модели обнаружения?
10. Какие этические и правовые аспекты применения ИИ в ИБ вы знаете?

Тема 9.2. Блокчейн-технологии и безопасность распределённых систем

1. Что такое распределённый реестр и чем блокчейн отличается от обычной базы данных?
2. Какие механизмы консенсуса вы знаете и какими свойствами обладают?
3. Какие криптографические примитивы лежат в основе блокчейн-технологий?
4. Что такое смарт-контракт и где хранится его код?

5. Какие типовые уязвимости смарт-контрактов вы знаете?
6. В чём суть уязвимости повторного входа (reentrancy)?
7. Как проводится аудит смарт-контрактов и что такое формальная верификация?
8. Какие атаки характерны для DeFi, блокчейн-мостов и оракулов?
9. Можно ли изменить код уже развёрнутого смарт-контракта?
10. Какие ограничения препятствуют применению блокчейна в корпоративных ИС?

Тема 9.3. Квантовая криптография и постквантовые алгоритмы

1. Почему развитие квантовых компьютеров угрожает классической асимметричной криптографии?
2. Что представляет собой атака «harvest now, decrypt later»?
3. Как устроен протокол BB84 и какие гарантии он обеспечивает?
4. Что такое квантовое распределение ключей (QKD) и каковы его ограничения?
5. Какие постквантовые алгоритмы стандартизированы NIST?
6. В чём различие между ML-KEM, ML-DSA и SLH-DSA?
7. Что такое гибридная схема шифрования и зачем она нужна?
8. Что такое крипто-agility и почему она важна при миграции?
9. С каких шагов начинается план миграции на постквантовую криптографию?
10. Какие работы в области постквантовой криптографии ведутся в России?

Тема 9.4. Автоматизация процессов ИБ и итоговая подготовка проекта

1. Что такое SOAR и чем он отличается от SIEM?
2. Что такое playbook и какие шаги включает типовой playbook реагирования?
3. Какие риски несёт полная автоматизация реагирования на инциденты?
4. Что такое DevSecOps и на каких этапах CI/CD встраиваются проверки безопасности?
5. Что такое инфраструктура как код и какие риски она создаёт?
6. Как автоматизировать управление уязвимостями и патч-менеджмент?
7. Какие метрики используют для оценки эффективности процессов ИБ?
8. Что должно входить в итоговый проект по защите информационной системы?
9. По каким критериям оценивается итоговый проект слушателя?
10. Какие направления развития автоматизации ИБ представляются вам наиболее перспективными?

Литература

Основная литература:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. — М.: ИНФРА-М, 2023.
2. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие. — М.: ФОРУМ: ИНФРА-М, 2022.
3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, киберзащита и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования.

Дополнительная литература:

1. OWASP Machine Learning Security Top 10 (owasp.org).
2. NIST SP 1800-38. Migration to Post-Quantum Cryptography.
3. SWC Registry: Smart Contract Weakness Classification and Test Cases (swcregistry.io).
4. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

Интернет-ресурсы:

1. Официальный сайт ФСТЭК России — fstec.ru.
2. Банк данных угроз безопасности информации ФСТЭК России — bdu.fstec.ru.
3. Национальный институт стандартов и технологий США (NIST) — csrc.nist.gov (проект постквантовой криптографии).
4. OWASP Foundation — owasp.org.
5. Официальный интернет-портал правовой информации — pravo.gov.ru.

Организационно-педагогические условия реализации программы

1) Применяемые образовательные технологии, формы и методы обучения, в том числе интерактивные:

В образовательном процессе используются разнообразные формы работы со слушателями.

- лекции, направленные на систематизирование основ теоретических знаний слушателей; лекции проводятся по наиболее сложным темам курса;
- практические задания – выполнение практико-ориентированных заданий по изучаемой теме для закрепления изученного материала на практических примерах с целью использования полученных навыков в будущей работе по специальности;
- тестирование – это стандартизированный метод оценки знаний, умений, навыков обучающихся.

2) Перечень информационных технологий, используемых при осуществлении образовательного процесса

Осуществляется проведение вебинаров для слушателей в удаленном доступе. Преподавателями используются работа в чате, индивидуальное консультирование слушателей.

Условия для функционирования электронной информационно-образовательной среды

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения
Система дистанционного обучения, система видеоконференцсвязи	Итоговая аттестация	Компьютер, подключенный к сети Интернет; интернет-браузер; Adobe Flash Player; Adobe Reader

3) Описание материально-технической базы, необходимой для осуществления

образовательного процесса

Технические средства обучения: компьютерный класс, оборудованный для проведения практических работ, персональными компьютерами, объединенными в сеть с выходом в Интернет.

Наименование специализированных учебных помещений	Вид занятий	Наименование оборудования, программного обеспечения
Учебный интерактивный тренажерный класс	Лекции Практические занятия	Мультимедийное оборудование, компьютеры, МФУ. Компьютер, подключенный к сети Интернет, интернет-браузер. Adobe Flash Player; Adobe Reader, ит.д.

Материально-технические условия соответствуют действующим санитарным и противопожарным правилам и нормам.

При проведении учебных занятий с применением дистанционных образовательных технологий (ДОТ) у слушателя должен быть персональный компьютер, с доступом в сеть интернет.

4) Кадровое обеспечение образовательного процесса.

Учебный процесс со слушателями обеспечивают преподаватели института, а также приглашенные специалисты и действующие практики других организаций.

Описание системы оценки качества освоения программы «Системный администратор Linux»

В систему оценки качества освоения программы «Системный администратор Linux» входят:

- текущий контроль по каждой теме, где предусмотрены практические занятия;
- промежуточная аттестация по каждому модулю;
- итоговая аттестация.

1. Методы текущего контроля:

- компьютерное тестирование.

Пример тестового вопроса текущего контроля:

Что означает показатель RPO (Recovery Point Objective) в контексте отказоустойчивости и высокой доступности?

- 1. Максимально допустимое время восстановления системы после сбоя.**
- 2. Максимально допустимая потеря данных (по времени) при сбое.**
- 3. Время автоматического переключения на резервный компонент (failover).**
- 4. Время возврата на основной компонент после устранения проблемы (failback).**

Порядок проведения: тестирование проводится с личного компьютера, 20 тестовых вопросов по каждой теме, 30 мин, количество попыток не ограничено.

Критерии оценивания: для получения зачета по теме необходимо набрать не

менее 60% от максимального количества баллов в любой попытке.

2. Порядок проведения итоговой аттестации:

• итоговое компьютерное тестирование (60 тестовых вопросов, 90 мин, количество попыток – 1).

Пример тестового вопроса для итоговой аттестации:

Какой архитектурный подход предполагает, что все узлы системы одновременно обрабатывают нагрузку, повышая производительность и отказоустойчивость?

1. *Active-Passive.*
2. *Standby-Redundant.*
3. *Active-Active.*
4. *Single-Node.*

Порядок проведения: тестирование проводится в компьютерном классе, 60 тестовых вопросов по каждому модулю, 90 мин, количество попыток – 1.

Критерии оценивания: результаты итоговой аттестации:

Набранное количество баллов (% от максимального значения)	Оценка (экзамен)
$<60\%$	неудовлетворительно
$60\% \leq 75\%$	удовлетворительно
$75\% \leq 85\%$	хорошо
$85\% \leq$	отлично

Разработчик программы _____ А.Е.Малыш