

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**ИО директора физтех-школы
радиотехники и компьютерных
технологий**

Д.А. Гаврилов

	Рабочая программа дисциплины (модуля)
по дисциплине:	Информационная безопасность
по направлению:	Инфокоммуникационные технологии и системы связи
профиль подготовки:	Телекоммуникационные сети и системы Физтех-школа Радиотехники и Компьютерных Технологий кафедра инфокоммуникационных систем и сетей
курс:	1
квалификация:	магистр

Семестры, формы промежуточной аттестации:

1 (осенний) - Дифференцированный зачет

2 (весенний) - Экзамен

Аудиторных часов: 75 всего, в том числе:

лекции: 60 час.

семинары: 15 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 75 час.

Подготовка к экзамену: 30 час.

Всего часов: 180, всего зач. ед.: 4

Программу составил: В.Г. Промыслов, канд. физ.-мат. наук, старший преподаватель

Программа обсуждена на заседании кафедры инфокоммуникационных систем и сетей 15.03.2022

Аннотация

Данный курс предназначен для получения студентами знаний о научно-исследовательской деятельности, практических навыков и компетенции в области фундаментальных и прикладных проблем информационной безопасности, таких как экспертиза, сертификация и контроль защищенности информации и объектов информатизации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации.

Курс состоит из двух частей рассчитанных на два семестра.

Первая часть курса позволит студентам овладеть необходимыми компетенциями и знаниями по современным подходам и методам общей теории информационной безопасности, познакомиться с формальными моделями, отражающими основные характеристики информационной безопасности реальных объектов и процессов.

Слушатели ознакомятся с основными практиками информационной безопасности принятыми в Российской Федерации и на международном уровне.

Вторая часть посвящена задаче анализа и разработки мер защиты систем и средств обработки информации, получают углубленные знания по математическим аспектам моделирования систем в части свойств информационной безопасности, научит студентов решать задачи синтеза и построения архитектуры безопасности современных цифровых систем управления и киберфизических систем.

Курс проводится в формате лекционных и семинарских занятий. Для успешного освоения курса необходимо посещение и конспектирование лекций, выполнение практических заданий на семинарах и самостоятельная работа с рекомендованной дополнительной литературой.

1. Цели и задачи

Цель дисциплины

Целью освоения дисциплины является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи дисциплины

- овладении профессиональными компетенциями в проектной деятельности, системного анализ в прикладной области, выявление угроз и оценке уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;
- обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- обучение студентов принципам разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;
- обучение студентов принципам разработки программ и методик, испытаний средств и систем обеспечения информационной безопасности;
- анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;
- формирование подходов к выполнению исследований студентами выполнение научных исследований с применением соответствующих физических и математических методов; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях в рамках выпускных работ на степень магистра.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации

УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.4 Способен использовать современные средства информационно-коммуникационных технологий для академического и профессионального взаимодействия
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности
	УК-6.2 Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами
ОПК-1 Способен представлять современную научную картину мира, выявлять естественнонаучную сущность проблем своей профессиональной деятельности, определять пути их решения и оценивать эффективность сделанного выбора	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные и прикладные научные знания в области естественных наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
ОПК-2 Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	ОПК-2.2 Владеет навыками реализации новых принципов и методов исследования в современных инфокоммуникационных системах и сетях
ОПК-3 Способен приобретать, обрабатывать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению задач своей профессиональной деятельности	ОПК-3.1 Умеет использовать современные информационные и компьютерные технологии, средства коммуникаций при поиске научно-технической информации в своей профессиональной деятельности

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

современные законы, стандарты, методы и технологии в области защиты информации;
формальные математические модели используемые для информационной безопасности;
требования к защите информации определенного типа;
основные угрозы в информационной безопасности;
средства и методы предотвращения и обнаружения вторжений;
требования к защите информации определенного типа;
современные законы, стандарты, методы и технологии в области защиты информации.
технические каналы утечки информации.

уметь:

эффективно использовать на практике теоретические компоненты науки: понятия, суждения, умозаключения, законы;
использовать современные программно-аппаратные средства защиты информации;
работать на современном экспериментальном оборудовании;
абстрагироваться от несущественных влияний при моделировании информационной безопасности реальных систем;
исследовать качественные и количественные характеристики систем;
подобрать и обеспечить защиту информации.

владеть:

владение современными методами обеспечения защиты информации;
навыками самостоятельной работы в лаборатории на современном экспериментальном оборудовании;
математическим моделированием информационных систем;
методами обоснования и выбора средств защиты информации.
навыками обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Введение в информационную безопасность	2			1
2	Правовое и организационное обеспечение информационной безопасности	2			1
3	Система менеджмента и оценки информационной безопасности	6			3
4	Программа безопасности. Политики, регламенты и процедуры безопасности.	4			2
5	Формальные модели безопасности	6			3
6	Безопасность в среде Web приложений.	2			1
7	Безопасность среды интерпретаторов и символьных вычислений.	2			1
8	Программные и аппаратные средства и методы обеспечения информационной безопасности	6			3
9	Криптографические методы защиты информации	2			4
10	Принципы безопасного программирования применительно к задачам информационной безопасности.	4	4		8
11	Модели угроз, анализ актуальных уязвимостей.	4	2		8
12	Безопасность сетевых протоколов и сервисов.	4			8
13	Методы и протоколы авторизации.	4			8
14	Механизмы безопасности на основе мандатных ссылок и разделения привилегий.	4	4		8
15	Безопасность виртуальной среды и облачных приложений	4	2		8
16	Классы защищенности и классификация активов	4	3		8
Итого часов		60	15		75
Подготовка к экзамену		30 час.			
Общая трудоёмкость		180 час., 4 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

1. Введение в информационную безопасность

Информационная безопасность. Основные понятия. Модели информационной безопасности. Информация в физическом и цифровом мире.

2. Правовое и организационное обеспечение информационной безопасности

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные международные и российские стандарты по информационной и кибербезопасности.

3. Система менеджмента и оценки информационной безопасности

Обзор процесса менеджмента риска информационной безопасности. Установление контекста. Организационная структура менеджмента риска информационной безопасности. Анализ риска.

Особенности оценки риска промышленных систем. Двухступенчатая процедура оценки риска на этапе разработки и проектирования. Методика оценки угроз ФСТЭК.

4. Программа безопасности. Политики, регламенты и процедуры безопасности.

Стадии и этапы программы безопасности. Политика безопасности уровня предприятия. Операционные регламенты. Архитектура безопасности, зоны и тракты.

5. Формальные модели безопасности

Дискреционная и мандатная и ролевая политики безопасности. Основные модели.

6. Безопасность в среде Web приложений.

Традиционная архитектура безопасности web сервера (Apache). Инъекции кода и команд. Межсайтовая подделка запросов и скрининг. Подделка запросов со стороны сервера. Обход механизмов аутентификации и авторизации.

7. Безопасность среды интерпретаторов и символьных вычислений.

Уязвимости интерпретаторов кода и типовые атаки на них (Perl, python, bash). Уязвимости «песочниц» выполнения бинарного кода.

8. Программные и аппаратные средства и методы обеспечения информационной безопасности

Защита информации от утечки по техническим каналам. Средства и методы защиты от сетевых компьютерных угроз. Технология межсетевых экранов. Технология обеспечения целостности данных на основе IMA/EVM. Реализация мандатной модели доступа SMACK.

9. Криптографические методы защиты информации

Криптографическая система, ее свойства. Симметричные и асимметричные системы шифрования. Цифровые подписи. Инфраструктура открытых ключей. Криптографические протоколы.

10. Принципы безопасного программирования применительно к задачам информационной безопасности.

Референтная модель управления памятью в компьютерах. Атаки на переполнение памяти в стек и динамически выделяемой области. Загрузка внешнего кода в исполняемую программу. Механизмы защиты и контроля памяти.

11. Модели угроз, анализ актуальных уязвимостей.

Угрозы и уязвимости (Модели ФСТЭК, и международные базы уязвимостей). Типовые сценарии атак. Порядок оценки угроз безопасности информации. Возможные объекты воздействия угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

12. Безопасность сетевых протоколов и сервисов.

Безопасность протоколов IP, UDP, TCP. Сканеры уязвимостей.

13. Методы и протоколы авторизации.

Задачи и методы аутентификации. Парольные методы аутентификации. Методы аутентификации использующие токены. Биометрические методы. Анализ и сравнение методов аутентификации. Протоколы аутентификации. Атака на протоколы. Модель обмена данными в каналах протокола аутентификации и атаки в канале. Многофакторная аутентификация.

14. Механизмы безопасности на основе мандатных ссылок и разделения привилегий.

Минимальные привилегии. Механизм безопасности UNIX, пользователи, процессы, файлы и файл дескрипторы, сетевые сервисы.

15. Безопасность виртуальной среды и облачных приложений

Модель безопасности в среде Docker контейнеров. Политика безопасности для виртуальной машины.

16. Классы защищенности и классификация активов

Категоризация и классификация активов. Основные классификаторы. Методы классификации.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная аудиторной доской.

6.Перечень рекомендуемой литературы

Основная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / Москва ; Берлин : Директ-Медиа, 2020. 270 с.
2. Девянин П. Н. Модели безопасности компьютерных систем.. Учеб. пособие для вузов. Москва: Академия, 2005. 144 с.
3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обуч. по направл. подгот. "Информ. безопасность" / В. В. Платонов. - 2-е изд., стер. - М. : Академия, 2014. - 336 с.

Дополнительная литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. – М.:Гелиос АРВ, 2002. – 380 с.: ил.
2. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с.
3. Смит Р.Э. Аутентификация: от паролей до открытых ключей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. –432 с.: ил.
4. Мао В. Современная криптография: теория и практика. :Пер. с англ. – М.: Издательский дом "Вильямс", 2005. –768 с.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // Методические материалы ФСТЭК. 2008.
6. Вострецова, Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / — Екатеринбург : Изд-во Урал. университета, 2019. — 204 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. Журналы по информационной безопасности, информационным технологиям, доступные через Internet.
2. Научные и научно-технические журналы: <http://scitation.aip.org/>, <http://www.sciencemag.org/>.
3. Электронные конспекты лекций, учебные пособия и сборники задач, разработанные для данного курса.
4. Документы и ресурсы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) <https://fstec.ru>.
5. <http://lib.mipt.ru> – электронная библиотека Физтеха.
6. <http://www.edu.ru> – федеральный портал «Российское образование».
7. <http://benran.ru> – библиотека по естественным наукам Российской академии наук.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Не используется

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения, понятия.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по конспектам лекций, учебной и научной литературе);
- подготовку к дифференцированному зачету и экзамену.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к преподавателю.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Инфокоммуникационные технологии и системы связи
профиль подготовки:	Телекоммуникационные сети и системы Физтех-школа Радиотехники и Компьютерных Технологий кафедра инфокоммуникационных систем и сетей
курс:	<u>1</u>
квалификация:	магистр

Семестры, формы промежуточной аттестации:

- 1 (осенний) - Дифференцированный зачет
- 2 (весенний) - Экзамен

Разработчик: В.Г. Промыслов, канд. физ.-мат. наук, старший преподаватель

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.4 Способен использовать современные средства информационно-коммуникационных технологий для академического и профессионального взаимодействия
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности
	УК-6.2 Оценивает свою деятельность, соотносит цели, способы и средства выполнения деятельности с её результатами
ОПК-1 Способен представлять современную научную картину мира, выявлять естественнонаучную сущность проблем своей профессиональной деятельности, определять пути их решения и оценивать эффективность сделанного выбора	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные и прикладные научные знания в области естественных наук
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
ОПК-2 Способен реализовывать новые принципы и методы исследования современных инфокоммуникационных систем и сетей различных типов передачи, распределения, обработки и хранения информации	ОПК-2.2 Владеет навыками реализации новых принципов и методов исследования в современных инфокоммуникационных системах и сетях
ОПК-3 Способен приобретать, обрабатывать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению задач своей профессиональной деятельности	ОПК-3.1 Умеет использовать современные информационные и компьютерные технологии, средства коммуникаций при поиске научно-технической информации в своей профессиональной деятельности

2. Показатели оценивания компетенций

В результате изучения дисциплины «Информационная безопасность» обучающийся должен:

знать:

современные законы, стандарты, методы и технологии в области защиты информации;
формальные математические модели используемые для информационной безопасности;
требования к защите информации определенного типа;
основные угрозы в информационной безопасности;
средства и методы предотвращения и обнаружения вторжений;
требования к защите информации определенного типа;
современные законы, стандарты, методы и технологии в области защиты информации.
технические каналы утечки информации.

уметь:

эффективно использовать на практике теоретические компоненты науки: понятия, суждения, умозаключения, законы;
использовать современные программно-аппаратные средства защиты информации;
работать на современном экспериментальном оборудовании;
абстрагироваться от несущественных влияний при моделировании информационной безопасности реальных систем;
исследовать качественные и количественные характеристики систем;
подобрать и обеспечить защиту информации.

владеть:

владение современными методами обеспечения защиты информации;
навыками самостоятельной работы в лаборатории на современном экспериментальном оборудовании;
математическим моделированием информационных систем;
методами обоснования и выбора средств защиты информации.
навыками обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Перечень контрольных вопросов для сдачи дифференцированного зачета:

Введение в информационная безопасность

1. Перечислите периоды информационного развития общества. Охарактеризуйте современный период развития информационного общества.
2. Дайте определение, что подразумевается под информационной безопасностью Российской Федерации.
3. Назовите предметную область теории информационной безопасности.
4. Назовите основные подходы, выделяемые в информационной безопасности. Охарактеризуйте значение обеспечения безопасности информации.
5. Перечислите перспективные направления информационной безопасности.
6. Какие вы знаете четыре основные задачи информационной безопасности.
7. Что принесла теория информации Шеннона для информационной безопасности.
8. Какое значение имеет информационная безопасность в жизни общества.
9. Дайте определения основным целям информационной безопасности, модель CIA (КИД).
10. Охарактеризуйте модель МакКамбера.
11. Охарактеризуйте гексагон Паркера.
12. Охарактеризуйте модель RMIAS.
13. Охарактеризуйте модель угроз Долева-Яо.
14. Сформулируйте основные принципы построения систем защиты.

Правовое и организационное обеспечение информационной безопасности

15. Дайте определение Информационной Безопасности по ГОСТ Р 50922-2006.
16. Дайте определение Информационной Безопасности по правовым документам.
17. Охарактеризуйте структуру и состав информационного законодательства.
18. Какие понятия в области информационной безопасности относятся к правовым? Перечислите и дайте определения. Какими основными документами они определяются в Российской Федерации?
19. Какие понятия в области информационной безопасности относятся к нормативным? Перечислите их и дайте определения. Какими основными документами они определяются в Российской Федерации?

20. Охарактеризуйте место информационной безопасности в стратегии национальной безопасности Российской Федерации.
 21. Дайте основные определения относящиеся к информационной безопасности установленные в федеральном законе «Об информации, информационных технологиях и о защите информации»
 22. Назовите типы информации в зависимости от порядка ее предоставления или распространения.
 23. Назовите виды защищаемой информации.
 24. Охарактеризуйте государственную национальную политику Российской Федерации в области информационной безопасности.
 25. Что такое персональные данные, профессиональная тайна, режим коммерческой тайны, государственная тайна?
 26. Охарактеризуйте процесс сертификации по информационной безопасности.
 27. Какие государственные органы занимаются сертификацией средств защиты информации?
 28. Охарактеризуйте процесс лицензирования средств защиты информации.
 29. Какие государственные органы занимаются лицензированием средств защиты информации?
 30. Какие основные международные стандарты в области информационной безопасности существуют?
 31. Какие основные стандарты РФ в области информационной безопасности существуют?
 32. Назовите основные стандарты по информационной безопасности для промышленных систем управления и сетей.
 33. Что такое правовая/техническая/физическая защита информации (по ГОСТ Р 50922-2006)?
 34. Перечислите основные документы ФСТЭК по информационной безопасности.
- Система менеджмента и оценки информационной безопасности
35. Охарактеризуйте процессный подход к информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 36. Дайте определения терминам: актив, доступность, конфиденциальность, целостность по ГОСТ Р ИСО/МЭК 27001.
 37. Дайте определения и охарактеризуйте отличие между событием и инцидентом информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 38. Дайте определение СМИБ по ГОСТ Р ИСО/МЭК 27001.
 39. Охарактеризуйте содержание разработки системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 40. Охарактеризуйте содержание внедрения и функционирования системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 41. Охарактеризуйте проведение мониторинга и анализа системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 42. Охарактеризуйте поддержку и улучшение системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 43. В чем заключается требования к документации при управлении информационной безопасностью по ГОСТ Р ИСО/МЭК 27001.
 44. Охарактеризуйте ответственность руководства организации при управлении информационной безопасностью по ГОСТ Р ИСО/МЭК 27001.
 45. Охарактеризуйте деятельность по аудиту системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 46. В чем заключается анализ системы менеджмента информационной безопасности со стороны руководства по ГОСТ Р ИСО/МЭК 27001.
 47. Охарактеризуйте деятельность по улучшению системы менеджмента информационной безопасности по ГОСТ Р ИСО/МЭК 27001.
 48. Перечислите девять принципов обеспечения информационной безопасности.
 49. Дайте определение и поясните содержание терминов доверие, профиль защиты, оценочный уровень доверия, оценка по ГОСТ Р ИСО 15408-1.
 50. Охарактеризуйте контекст для оценок информационной безопасности устанавливаемый по ГОСТ Р ИСО 15408-1.
 51. Охарактеризуйте общий контекст безопасности устанавливаемый по ГОСТ Р ИСО 15408-1.
 52. Охарактеризуйте Понятия, используемые при оценке информационной безопасности, и их взаимосвязь по ГОСТ Р ИСО 15408-1.
 53. Охарактеризуйте процесс оценки ОО по ГОСТ Р ИСО 15408-1.

54. Охарактеризуйте последовательное формирование требований и спецификаций по ГОСТ Р ИСО 15408-1.
55. Охарактеризуйте организацию и структуру требований информационной безопасности по ГОСТ Р ИСО 15408-1.
56. Охарактеризуйте профиль защиты по ГОСТ Р ИСО 15408-1.
57. Охарактеризуйте содержание задания по безопасности по ГОСТ Р ИСО 15408-1.
58. Перечислите основное применение ФТБ по ГОСТ Р ИСО 15408-2.
59. Опишите структуру функционального класса и семейства по ГОСТ Р ИСО 15408-2.
60. Охарактеризуйте основные классы функциональных требований по ГОСТ Р ИСО 15408-2.
61. Перечислите основные причины уязвимостей информационной безопасности по ГОСТ Р ИСО 15408-3.
62. Дайте определение и охарактеризуйте доверие и оценку доверия по ГОСТ Р ИСО 15408-3.
63. Охарактеризуйте шкалу оценки доверия по ГОСТ Р ИСО 15408-3.
64. Охарактеризуйте оценочные уровни доверия по ГОСТ Р ИСО 15408-3 3.
- Программа безопасности. Политики, регламенты и процедуры безопасности
65. Дайте определение политике безопасности, процедурам безопасности и программе безопасности по ГОСТ Р 56205-2014.
66. Охарактеризуйте политику информационной безопасности высокого уровня. Приведите ее примерное содержание.
67. Охарактеризуйте политику информационной безопасности уровня предприятия по ГОСТ Р 56205-2014.
68. Охарактеризуйте операционные политики и регламенты по ГОСТ Р 56205-2014.
69. Охарактеризуйте задачи, решаемые с помощью политик и регламентов по ГОСТ Р 56205-2014.
70. Дайте определения уровня, зоны, тракта, границы, коммуникационного пути, демилитаризованной зоны в соответствии с ГОСТ Р 56205-2014. Приведите их примеры.

Оценка рисков информационной безопасности

71. Дайте определения риска информационной безопасности, предотвращения риска, коммуникации риска, количественной оценки риска, идентификации риска, снижения риска, сохранения риска, переноса риска, по ГОСТ Р ИСО 27005.
72. Опишите взаимосвязь компонентов информационной безопасности в контексте оценки риска.
73. Назовите и охарактеризуйте возможные стратегии управления рисками по ГОСТ Р ИСО 27005.
74. Приведите краткое описание возможных методов оценки риска и их классификацию по стандарту ГОСТ Р ИСО/МЭК 31010.
75. Охарактеризуйте процесс менеджмента риска информационной безопасности по ГОСТ Р ИСО 27005.
76. Охарактеризуйте установление контекста при оценке риска информационной безопасности по ГОСТ Р ИСО 27005.
77. Охарактеризуйте анализ риска при оценке риска информационной безопасности по ГОСТ Р ИСО 27005.
78. Охарактеризуйте оценку риска информационной безопасности по ГОСТ Р ИСО 27005.
79. Опишите, что такое остаточный риск и процесс принятия риска информационной безопасности по ГОСТ Р ИСО 27005.
80. Приведите примеры типичных угроз и охарактеризуйте их по ГОСТ Р ИСО 27005.
81. Приведите примеры типичных уязвимостей и методы их оценки и охарактеризуйте их по ГОСТ Р ИСО 27005.
82. Какие исходные данные используются для оценки угроз безопасности информации по методике оценки угроз ФСТЭК?
83. Что включает определение сценариев реализации угрозы на этапе эксплуатации по методике оценки угроз ФСТЭК?
84. Приведите пример сценария реализации угрозы безопасности информации по методике оценки угроз ФСТЭК?
85. Приведите пример содержания модели угроз безопасности информации по методике оценки угроз ФСТЭК?

86. Охарактеризуйте этапы оценки угроз безопасности по методике оценки угроз ФСТЭК?
87. Перечислите виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации.
88. Приведите примеры определения объектов воздействия и видов воздействия на них по методике оценки угроз ФСТЭК.
89. Перечислите возможные цели реализации угроз безопасности информации нарушителем по методике оценки угроз ФСТЭК.
- Программа безопасности. Политики, регламенты и процедуры безопасности
90. Дайте определение политике безопасности, процедурам безопасности и программе безопасности по ГОСТ Р 56205-2014.
91. Охарактеризуйте политику информационной безопасности высокого уровня. Приведите ее примерное содержание.
92. Охарактеризуйте политику информационной безопасности уровня предприятия по ГОСТ Р 56205-2014.
93. Охарактеризуйте операционные политики и регламенты по ГОСТ Р 56205-2014.
94. Охарактеризуйте задачи, решаемые с помощью политик и регламентов по ГОСТ Р 56205-2014.
95. Охарактеризуйте зоны безопасности в соответствии с ГОСТ Р 56205-2014.
96. Охарактеризуйте тракты безопасности в соответствии с ГОСТ Р 56205-2014.

Формальные модели безопасности

97. Приведите определение решетки MLS.
98. Охарактеризуйте, что представляет собой модель пятимерного пространства Хартсона.
99. Охарактеризуйте процесс организации доступа в пятимерном пространстве Хартсона.
100. Охарактеризуйте элементы модели ХРУ.
101. Расскажите об анализе безопасности в системе ХРУ.
102. Охарактеризуйте элементы классической модели take-grant.
103. Охарактеризуйте санкционированное получение прав доступа в классической модели take-grant.
104. Расскажите о похищении прав доступа в классической модели take-grant.
105. Охарактеризуйте элементы расширенной модели take-grant.
106. Расскажите о санкционированном получении прав доступа в расширенной модели take-grant.
107. Расскажите о похищении прав доступа в расширенной модели take-grant.
108. Охарактеризуйте элементы классической модели Белла—ЛаПадула.
109. Охарактеризуйте свойства безопасности модели Белла—ЛаПадула, включая теоремы.
110. Опишите реализацию политики low-watermark в модели Белла—ЛаПадула.
111. Охарактеризуйте модель RBAC0.
112. Охарактеризуйте модель RBAC1.
113. Охарактеризуйте модель RBAC2.
114. Охарактеризуйте модель RBAC3.
115. Охарактеризуйте элементы модели администрирования РРД.
116. Охарактеризуйте группы административных ролей РРД и администрирование множеств авторизованных ролей пользователей.
117. Охарактеризуйте администрирование множеств прав доступа, которыми обладают роли в модели РРД.
118. Охарактеризуйте администрирование иерархии ролей в РРД.
119. Охарактеризуйте виды скрытых каналов утечки информации и приведите их примеры.

Программные и аппаратные средства и методы обеспечения информационной безопасности

120. Назовите основные виды мер защиты информации. Приведите примеры конкретных мер для каждого вида.
121. Расскажите о принципе эшелонированной защиты.
122. Что такое вредоносная программа. Перечислите основные типы вредоносных программ
123. Алгоритм Монтгомери. Два основных принципа фильтрации пакетов. Какой из них предпочтительней и почему.

124. Расскажите о технологии обеспечения целостности данных на основе IMA/EVM.
 125. Расскажите о реализации мандатной модели доступа SMACK.
- Безопасность в среде Web приложений.
126. Расскажите об архитектуре безопасности web сервера (Apache).
 127. Охарактеризуйте атаки инъекции кода и команд. Что такое Межсайтовая подделка запросов и скрининг?
 128. Охарактеризуйте подделку запросов со стороны сервера. Приведите пример обхода механизмов аутентификации и авторизации.
- Безопасность среды интерпретаторов и символьных вычислений.
129. Охарактеризуйте типичные уязвимости интерпретаторов кода и типовые атаки на них (Perl, python, bash).
 130. Охарактеризуйте типичные уязвимости «песочниц» выполнения бинарного кода, типовые атаки на них.

Перечень контрольных вопросов для сдачи экзамена:

Криптографические методы защиты информации

1. Что такое криптографическая система. Свойства криптографической системы. Требования к криптографической системе.
2. Какие используются симметричные алгоритмы шифрования. Расскажите об алгоритме DES. Сеть Фейстеля (Файстеля).
3. Расскажите про уязвимости классического алгоритма DES, Тройной алгоритм DES.
4. Какие используются ассиметричные алгоритмы шифрования. Протокол обмена открытыми ключами. Стойкость протокола Диффи-Хеллмана.
5. Расскажите об алгоритме шифрования RSA. Уязвимости учебного RSA.
6. Расскажите об особенностях реализации алгоритма RSA (Sliding window, CRT, Алгоритм Монтгомери).
7. Что такое криптографическая хеш-функция. Какие используются криптографические хеш-функции.
8. Расскажите про механизм цифровой подписи.
9. Расскажите про инфраструктуру открытых ключей.
10. Какие российские и международные стандарты на формирование цифровой подписи существуют.

Принципы безопасного программирования применительно к задачам информационной безопасности.

11. Расскажите об организации памяти x86, организации вызова стека cdecl. Какие атаки на стек возможны. Охарактеризуйте их.
12. Расскажите какие методы защиты от атак переполнения буфера памяти вы знаете?

Модели угроз, анализ актуальных уязвимостей.

13. Охарактеризуйте работу аналитика в MITRE ATT&CK. Приведите примеры описания техник проникновения в MITRE ATT&CK.
14. Опишите классификацию угроз безопасности персональных данных в модели ФСТЭК.
15. Охарактеризуйте элементы описания угроз в модели ФСТЭК.

Безопасность сетевых протоколов и сервисов. Безопасность протоколов IP, UDP, TCP. Сканеры уязвимостей.

16. Охарактеризуйте уязвимости отдельных протоколов стека протоколов TCP/IP по модели ФСТЭК.
17. Расскажите про уязвимости протокола IP
18. Расскажите про сканеры уязвимостей. Приведите примеры сценариев работы со сканером уязвимостей и анализ результатов работы.

Методы и протоколы авторизации.

19. Расскажите о задаче и методах аутентификации.
20. Охарактеризуйте парольные методы аутентификации.
21. Охарактеризуйте методы аутентификации использующие токены.
22. Охарактеризуйте биометрические методы.

23. Проведите сравнение методов аутентификации.
24. Охарактеризуйте протоколы аутентификации.
25. Охарактеризуйте атака на протоколы аутентификации.
26. Охарактеризуйте Модель обмена данными в каналах протокола аутентификации и атаки в канале..
27. Охарактеризуйте и приведите примеры многофакторной аутентификации
- Механизмы безопасности на основе мандатных ссылок и разделения привилегий
28. Охарактеризуйте механизм безопасности UNIX, пользователи, процессы, сетевые сервисы.
29. Охарактеризуйте механизм безопасности UNIX файлы и файл дескрипторы.
- Безопасность виртуальной среды и облачных приложений
30. Расскажите о модели безопасности в среде Docker контейнеров.
31. Охарактеризуйте политику безопасности для виртуальной машины в облачной среде.
- Классы защищенности и классификация активов
32. Перечислите уровни автоматизированной системы управления.
33. Чем достигается защита информации в автоматизированной системе управления?
34. Сколько классов защищённости определяет документ ФСТЭК Приказ 31? .
35. Кому может быть назначен класс защищённости?
36. Где указываются требования к классу защищенности?
37. Когда пересматривается класс защищенности?
38. Что необходимо учитывать при определении угроз безопасности информации?
39. Чем определяются и что содержат требования к системе защиты автоматизированной системы управления?
40. Какие этапы включает разработка системы защиты автоматизированной системы управления, осуществляемая в соответствии с техническим заданием?
41. Что нужно определить при проектировании системы защиты автоматизированной системы управления?
42. Что должна содержать эксплуатационная документация на систему защиты автоматизированной системы управления?
43. Какие этапы включает внедрение системы защиты автоматизированной системы управления?
44. Что должны включать разрабатываемые организационно-распорядительные документы по защите информации (политики)?
45. Какие этапы включают испытания системы защиты автоматизированной системы управления?
46. Что включает анализ уязвимостей автоматизированной системы управления?
47. Что используется в качестве исходных данных при приемочных испытаниях системы защиты автоматизированной системы управления?
48. Какие процедуры включает обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления?
49. Что входит в управление (администрирование) системой защиты автоматизированной системы управления?
50. Что входит в управление конфигурацией автоматизированной системы управления и ее системы защиты на этапе эксплуатации?
51. Что включает обеспечение защиты информации при выводе из эксплуатации автоматизированной системы?
52. Что должны обеспечить организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты?
53. Что включает выбор мер защиты информации для их реализации в автоматизированной системе управления в рамках ее системы защиты?
54. Какие действия необходимо осуществить при отсутствии возможности реализации отдельных мер защиты?
55. Что должны минимально обеспечивать выбранные и реализованные в автоматизированной системе управления в рамках ее системы защиты меры защиты информации (по классам защищенности)?
56. Как определяется класс защищенности автоматизированной системы управления (с учетом конфиденциальности)?

57. Как определяется класс защищенности автоматизированной системы управления (без учета конфиденциальности)?

58. Охарактеризуйте уровни безопасности в соответствии с ГОСТ Р 56205-2014.

Примеры билетов для проведения экзамена:

Билет №1.

1. Что такое криптографическая система. Свойства криптографической системы. Требования к криптографической системе.
2. Опишите классификацию угроз безопасности персональных данных в модели ФСТЭК.
3. Расскажите об организации памяти x86, организации вызова стека cdecl. Какие атаки на стек возможны. Охарактеризуйте их.

Билет №2.

1. Какие используются асимметричные алгоритмы шифрования. Протокол обмена открытыми ключами. Стойкость протокола Диффи-Хеллмана.
2. Расскажите какие методы защиты от атак переполнения буфера памяти вы знаете?
3. Расскажите о задаче и методах аутентификации.

Критерии оценивания

Оценка отлично (10) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (9) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (8) выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо (7) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо (6) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо (5) выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно (4) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно (3) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно (2) выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно (1) выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Экзамен и дифференцированный зачет проводится в устной форме.

При проведении устного дифференцированного зачета и экзамена обучающемуся предоставляется 1 час на подготовку. Опрос обучающегося по билету на устном экзамене не должен превышать двух астрономических часов.

Во время проведения экзамен и дифференцированного зачета обучающиеся могут пользоваться программой дисциплины.