

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

УТВЕРЖДЕНО

**Проректор по учебной работе и
довузовской подготовке**

А.А. Воронов

	Рабочая программа дисциплины (модуля)
по дисциплине:	Безопасность информационных технологий
по направлению:	Информатика и вычислительная техника
профиль подготовки:	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра информатики и вычислительной математики
курс:	1
квалификация:	магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 0 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Программу составил: И.Т. Кадошук, канд. физ.-мат. наук, доцент, доцент

Программа обсуждена на заседании кафедры информатики и вычислительной математики 17.02.2023

Аннотация

Целью курса является знакомство студентов с понятием безопасности информационных систем и обучение их навыкам проектирования систем информационной безопасности корпоративных автоматизированных информационных систем. Обучающиеся узнают основы организации и управления информационной безопасностью, оценки рисков. Будет основано введение в криптографические методы.

1. Цели и задачи

Цель дисциплины

- освоение студентами знаний в области методологии проектирования систем информационной безопасности корпоративных автоматизированных информационных систем.

Задачи дисциплины

- Освоение студентами знаний в области архитектур систем информационной безопасности и защиты информации;
- изучение и анализ основных классов требований к информационным автоматизированным системам с точки зрения информационной безопасности и защиты критических данных корпоративного бизнеса;
- освоение методологии проектирования корпоративных систем информационной безопасности и защиты информации, реализуемой посредством пакета нормативно-регламентирующей документации;
- знакомство со всеми базовыми классами средств защиты информации;
- изучение архитектур основных защищенных протоколов и криптографических алгоритмов;

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области информатики и вычислительной техники	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области информатики и вычислительной техники
	ОПК-1.3 Понимает междисциплинарные связи в области информатики и вычислительной техники и способен их применять при решении задач профессиональной деятельности
ПК-2 Понимает и способен применить в научно-исследовательской и прикладной деятельности основные законы естествознания, современный математический аппарат и алгоритмы, современные информационно-коммуникационные технологии	ПК-2.1 Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения
	ПК-2.2 Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности
	ПК-2.4 Владеет методами и алгоритмами решения задач цифровой обработки сигналов, использования сети Интернет, аннотирования, реферирования, библиографического поиска, опыт работы с научными источниками
ПК-1 Готов к включению в профессиональное сообщество; способен	ПК-1.2 Умеет решать научные задачи с пониманием существующих подходов к верификации моделей программного обеспечения в связи с поставленной целью и в соответствии с выбранной методикой

проводить под научным руководством локальные исследования на основе существующих методов в конкретной области профессиональной деятельности

ПК-1.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации; владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- Основные понятия и категории в области «Безопасности информационных технологий»;
- типы и категории информации, проблемы информационной защиты;
- базовые понятия политики безопасности, уязвимости, атаки, риски, потенциальные потери и средства защиты;
- основы управления информационной безопасностью;
- основные нормативно-директивные документы, регулирующие все аспекты организации и управления информационной безопасностью;
- основы методики управления рисками информационной безопасности;
- базовые понятия методик оценки рисков информационной безопасности;
- основные требования информационной безопасности;
- основные криптографические системы, алгоритмы и методы шифрования информации;
- базовые средства защиты операционных систем;
- основные методы управления доступом и управления правами пользователей;
- принципы и методы защиты программного обеспечения;
- основные уязвимости сетевой безопасности;
- классы средств сетевой безопасности;
- основные протоколы безопасности Интернет;
- архитектура IP VPN. Архитектура IPSec. Протоколы IPSec. Протокол генерации и обмена ключей IKE;
- принципы управления ключами шифрования;
- архитектуру инфраструктуры распределения открытых ключей.

уметь:

- Подготовить корпоративную политику информационной безопасности;
- подготовить корпоративную Концепцию информационной безопасности;
- сформировать модель потенциального нарушителя корпоративной автоматизированной информационной системы;
- оценить риски информационной безопасности;
- подобрать меры снижения идентифицированных рисков информационной безопасности;
- сформулировать адекватные требования к различным категориям корпоративных данных и информации с точки зрения информационной безопасности;
- использовать криптографические алгоритмы, методы и подходы к защите конфиденциальных данных;
- подготовить проект Политики информационной защиты корпоративных операционных систем;
- подготовить проект Политики управления доступом и распределением прав пользователей;
- подготовить проект Политики защиты программного обеспечения;
- подготовить проект Политики сетевой защиты корпоративной информационной системы;
- осуществить адекватный выбор сетевых средств и методов защиты для снижения рисков сетевой информационной безопасности;
- подготовить проект Политики управления ключами шифрования корпоративной информационной системы;
- подготовить проект системы информационной безопасности корпоративной системы поддержки учебного процесса высшего учебного заведения;
- подготовить проект системы информационной безопасности корпоративной системы лечебного учреждения (поликлиники, больницы);
- подготовить проект системы информационной безопасности корпоративной автоматизированной системы кредитной организации;
- подготовить проект системы информационной безопасности корпоративной системы информационно-автоматизированной системы интернет-компании.

владеть:

- Методикой проектирования системы информационной безопасности в рамках корпоративной автоматизированной информационной системы поддержки бизнес-операций;
- методикой оценки и управления рисками информационной безопасности в рамках корпоративной автоматизированной информационной системы;
- основными методиками управления доступом и правами пользователей.

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	Что такое «информационная безопасность»? Почему мы тратим время на курс «основы информационной безопасности»?		2		2
2	Основные положения и методика информационной защиты.		4		2
3	Организация и управление информационной безопасностью.		2		2
4	Оценка и управление рисков.		4		2
5	Типы требований информационной безопасности.		2		2
6	Введение в криптографические методы.		4		5
7	Защита операционных систем.		2		
8	Сетевая безопасность.		2		
9	Распространение, сертификация, управление ключами.		2		
10	Среда открытых систем POSIX.		2		
11	Безопасность услуг человеко-машинного интерфейса. Система X-Windows.		2		
12	Безопасность сервисов управления данными.		2		
Итого часов			30		15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

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

Семестр: 2 (Весенний)

1. Что такое «информационная безопасность»? Почему мы тратим время на курс «основы информационной безопасности»?

Что такое «информационная безопасность»? Почему мы тратим время на курс «основы информационной безопасности»? Типы информации, проблемы защиты и краткий исторический экскурс. Что защищают и от кого? Краткое содержание курса, основные цели и задачи, главные результаты, задания и отчетность.

2. Основные положения и методика информационной защиты.

Основные положения и методика информационной защиты. Политики безопасности, уязвимости, атаки, риски, потенциальные потери и средства защиты. Терминология. Различные подходы и методика управления информационной безопасностью.

3. Организация и управление информационной безопасностью.

Организация и управление информационной безопасностью. Организационные структуры. Категории и классификация информации. Стандартизирующие документы и организации.

4. Оценка и управление рисков.

Оценка и управление рисков. Уязвимости и оценка потенциальных потерь.

5. Типы требований информационной безопасности.

Типы требований информационной безопасности. Типы требований информационной безопасности и соответствующие методы обеспечения.

6. Введение в криптографические методы.

Введение в криптографические методы. Обзор алгоритмов и подходов к шифрованию: потоковые и блочные алгоритмы, симметричные и асимметричные системы, цифровая подпись и хэш-функции. Национальные особенности криптографических систем.

7. Защита операционных систем.

Защита операционных систем. Базовые средства – аутентификация, защита файловых систем, взаимодействие с внешними системами. Защита программного обеспечения – целостность..

8. Сетевая безопасность.

Сетевая безопасность. Основные уязвимости. Классы средств сетевой безопасности. Межсетевые экраны. Сетевые протоколы безопасности Интернет. Защищенные виртуальные сети. Протоколы IP VPN. Архитектура IP VPN. Архитектура IPSec. Протоколы IPSec. Протокол генерации и обмена ключей IKE.

9. Распространение, сертификация, управление ключами.

Распространение, сертификация, управление ключами. Public Key Infrastructure Услуги третьей доверенной стороны и распределение ключей.

10. Среда открытых систем POSIX.

Среда открытых систем POSIX. Безопасность сервисов операционных систем. Функциональность. Аудит. Управление доступом в систему. Привилегии. Информационные метки. Защита и управление утилитами.

11. Безопасность услуг человеко-машинного интерфейса. Система X-Windows.

Безопасность услуг человеко-машинного интерфейса. Система X-Windows.

12. Безопасность сервисов управления данными.

Безопасность сервисов управления данными. Поддержка криптографических баз данных.
Заключение. Чему мы научились? Обсуждение результатов самостоятельных работ

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

Необходимое оборудование для практических занятий: компьютер и мультимедийное оборудование (проектор, звуковая система)

6.Перечень рекомендуемой литературы

Основная литература

1. Защита информации [Текст] : учеб. пособие для вузов / Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т .— М. : МФТИ, 2011 .— 262 с.

Дополнительная литература

1. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин .— М. : ДМК Пресс, 2012 .— Электрон. версия печ. публикации .

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

Электронные конспекты лекций и другие учебные материалы размещаются на сайте <http://www.ihed.ras.ru/norman/student/1-grid2.php>.

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

Необходимое программное обеспечение: программы управления презентациями MS Powerpoint, программа Acrobat Reader.

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

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

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, подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;
- решение задач, предлагаемых студентам на практических занятиях и в качестве курсового задания,
- подготовку к практическим занятиям, дифференцированному зачёту.

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

Показателем владения материалом служит умение решать задачи.

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Информатика и вычислительная техника
профиль подготовки:	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра информатики и вычислительной математики
курс:	<u>1</u>
квалификация:	магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

Разработчик: И.Т. Кадошук, канд. физ.-мат. наук, доцент, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Владеет системой фундаментальных научных знаний в области информатики и вычислительной техники	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области информатики и вычислительной техники
	ОПК-1.3 Понимает междисциплинарные связи в области информатики и вычислительной техники и способен их применять при решении задач профессиональной деятельности
ПК-2 Понимает и способен применить в научно-исследовательской и прикладной деятельности основные законы естествознания, современный математический аппарат и алгоритмы, современные информационно-коммуникационные технологии	ПК-2.1 Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения
	ПК-2.2 Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности
	ПК-2.4 Владеет методами и алгоритмами решения задач цифровой обработки сигналов, использования сети Интернет, аннотирования, реферирования, библиографического поиска, опыт работы с научными источниками
ПК-1 Готов к включению в профессиональное сообщество; способен проводить под научным руководством локальные исследования на основе существующих методов в конкретной области профессиональной деятельности	ПК-1.2 Умеет решать научные задачи с пониманием существующих подходов к верификации моделей программного обеспечения в связи с поставленной целью и в соответствии с выбранной методикой
	ПК-1.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации; владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке

2. Показатели оценивания компетенций

В результате изучения дисциплины «Безопасность информационных технологий» обучающийся должен:

знать:

- Основные понятия и категории в области «Безопасности информационных технологий»;
- типы и категории информации, проблемы информационной защиты;
- базовые понятия политики безопасности, уязвимости, атаки, риски, потенциальные потери и средства защиты;
- основы управления информационной безопасностью;
- основные нормативно-директивные документы, регулирующие все аспекты организации и управления информационной безопасностью;
- основы методики управления рисками информационной безопасности;
- базовые понятия методик оценки рисков информационной безопасности;
- основные требования информационной безопасности;
- основные криптографические системы, алгоритмы и методы шифрования информации;
- базовые средства защиты операционных систем;
- основные методы управления доступом и управления правами пользователей;
- принципы и методы защиты программного обеспечения;
- основные уязвимости сетевой безопасности;
- классы средств сетевой безопасности;
- основные протоколы безопасности Интернет;
- архитектура IP VPN. Архитектура IPSec. Протоколы IPSec. Протокол генерации и обмена ключей IKE;
- принципы управления ключами шифрования;
- архитектуру инфраструктуры распределения открытых ключей.

уметь:

- Подготовить корпоративную политику информационной безопасности;
- подготовить корпоративную Концепцию информационной безопасности;
- сформировать модель потенциального нарушителя корпоративной автоматизированной информационной системы;
- оценить риски информационной безопасности;
- подобрать меры снижения идентифицированных рисков информационной безопасности;
- сформулировать адекватные требования к различным категориям корпоративных данных и информации с точки информационной безопасности;
- использовать криптографические алгоритмы, методы и подходы к защите конфиденциальных данных;
- подготовить проект Политики информационной защиты корпоративных операционных систем;
- подготовить проект Политики управления доступом и распределением прав пользователей;
- подготовить проект Политики защиты программного обеспечения;
- подготовить проект Политики сетевой защиты корпоративной информационной системы;
- осуществить адекватный выбор сетевых средств и методов защиты для снижения рисков сетевой информационной безопасности;
- подготовить проект Политики управления ключами шифрования корпоративной информационной системы;
- подготовить проект системы информационной безопасности корпоративной системы поддержки учебного процесса высшего учебного заведения;
- подготовить проект системы информационной безопасности корпоративной системы лечебного учреждения (поликлиники, больницы);
- подготовить проект системы информационной безопасности корпоративной автоматизированной системы кредитной организации;
- подготовить проект системы информационной безопасности корпоративной системы информационно-автоматизированной системы интернет-компании.

владеть:

- Методикой проектирования системы информационной безопасности в рамках корпоративной автоматизированной информационной системы поддержки бизнес-операций;
- методикой оценки и управления рисками информационной безопасности в рамках корпоративной автоматизированной информационной системы;
- основными методиками управления доступом и правами пользователей.

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

Текущий контроль освоения материала студентами проводится с помощью периодических опросов на семинарах. Примеры контрольных вопросов:

- Назовите различные подходы и методика управления информационной безопасностью.
- Назовите основные категории и классификация информации.
- Перечислите основные типы требований информационной безопасности.
- В чём отличия симметричных и асимметричных систем шифрования.
- Приведите пример используемой на практике хэш-функции.
- Назовите базовые методы защиты операционных систем.
- Назовите основные различия IP VPN и IPSec.
- Объясните назначение "привилегий" в контексте открытых систем.
- Перечислите основные компоненты системы X-Windows.
- Назовите основные этапы обеспечения безопасности сервисов управления данными.

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

1. Что такое «информационная безопасность»?
2. В чем состоит методика информационной защиты?
3. Что такое политики безопасности?
4. Какие подходы и методики управления информационной безопасностью вы знаете?
5. Расскажите об организационных структурах и составе стандартизирующих документов.
6. Что такое категоризация? Чем отличаются категории друг от друга? В чем отличия категоризации от классификации информации?
7. Расскажите о методике управления рисками в информационной безопасности.
8. Что такое уязвимости и как оценить потенциальные потери?
9. Какие типы требований информационной безопасности существуют? Перечислить. Охарактеризовать.
10. Какие типы криптографических алгоритмов вы знаете?
11. Что такое симметричные и асимметричные системы шифрования?
12. Что такое цифровая подпись и хэш-функции. Общее и различия?
13. Национальные (государственные) особенности криптографических систем?
14. Перечислить типы средств защиты операционных систем?
15. Объясните принципы защиты прикладного программного обеспечения?
16. Перечислить классы средств сетевой безопасности. Охарактеризовать каждый из классов.
17. Опишите архитектуру IP VPN по всем уровням сетевых взаимодействий?
18. Перечислить протоколы IP VPN по всем уровням сетевых взаимодействий?
19. Расскажите об архитектуре IPSec.
20. Перечислите все протоколы в архитектуре IPSec.
21. Расскажите о протоколах идентификации в архитектуре IPSec.
22. Расскажите о протоколах шифрования в архитектуре IPSec.
23. Расскажите о протоколах генерации и обмена ключей IKE.
24. Что такое инфраструктура открытых ключей (PKI – public key infrastructure)? Опишите архитектуру PKI, основные компоненты.
25. В чем состоят услуги третьей доверенной стороны при распределении ключей.
26. Расскажите о типах управления доступом и распределения прав.
27. Расскажите о безопасности сервисов человеко-машинного интерфейса
28. Расскажите о специфике поддержки криптографических баз данных.

Критерии оценивания

Оценка «отлично (10)» выставляется обучающемуся, если показавшему всесторонние, систематизированные, глубокие знания предмета и в ходе беседы он верно и детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «отлично (9)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня (мог не ответить на некоторые уточняющие вопросы). Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «отлично (8)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на четыре (4) произвольных вопроса из выше приведенного перечня (не ответил на уточняющие вопросы).

Оценка «хорошо (7)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на три (3) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «хорошо (6)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на три (3) произвольных вопроса из выше приведенного перечня (не ответил на некоторые уточняющие вопросы). Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «хорошо (5)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на два (2) произвольных вопроса из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы.

Оценка «удовлетворительно (4)» выставляется обучающемуся, если в ходе беседы он верно и достаточно детально ответил на один (1) произвольный вопрос из выше приведенного перечня. Детальный ответ предполагает верные ответы на все уточняющие вопросы. Подготовка и защита инициативной курсовой работы является преимуществом.

Оценка «удовлетворительно (3)» выставляется обучающемуся, если в ходе беседы он верно, но не исчерпывающее детально ответил на один (1) произвольный вопрос из выше приведенного перечня (не ответил на уточняющие вопросы).

Оценка «неудовлетворительно (2)» выставляется обучающемуся, если в ходе беседы он не смог ответить ни на один произвольный вопрос из выше приведенного перечня, но смог ответить на наводящие вопросы и вопросы с «подсказками».

Оценка «неудовлетворительно (1)» выставляется обучающемуся, если в ходе беседы он не смог ответить ни на один произвольный вопрос из выше приведенного перечня, а также ни на один наводящий вопрос.

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

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины, а также собственными конспектами занятий по предмету.

Дифференцированный зачет проводится по итогам текущей активности в ходе занятий и путем организации специального опроса, проводимого в простой устной форме, в виде беседы преподавателя и студента.