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

«УТВЕРЖДАЮ
Проректор по учебной работе
и экономическому развитию
_____ Д.А. Зубцов

Рабочая программа дисциплины (модуля)

по дисциплине: Безопасность информационных технологий
по направлению: Прикладные математика и физика (магистратура)
профиль подготовки: Математические и информационные технологии
Факультет управления и прикладной математики
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.
практические и семинарские занятия: 30 час.
лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

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

Программа обсуждена на заседании кафедры

17 мая 2016 г.

СОГЛАСОВАНО:

Заведующий кафедрой И.Б. Петров

Начальник учебного управления И.Р. Гарайшина

Декан факультета А.А. Шананин

1. Цели и задачи

Цель дисциплины

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

Задачи дисциплины

1) Освоение студентами знаний в области архитектур систем информационной безопасности и защиты информации.

2) Изучение и анализ основных классов требований к информационным автоматизированным системам с точки зрения информационной безопасности и защиты критических данных корпоративного бизнеса.

3) Освоение методологии проектирования корпоративных систем информационной безопасности и защиты информации реализуемой посредством пакета нормативно-регламентирующей документации.

4) Знакомство со всеми базовыми классами средств защиты информации.

5) Изучение архитектур основных защищенных протоколов и криптографических алгоритмов.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Безопасность информационных технологий» относится к вариативной части образовательной программы.

Дисциплина «Безопасность информационных технологий» базируется на дисциплинах:

Дифференциальные уравнения;

Математический анализ;

Информатика.

Дисциплина «Безопасность информационных технологий» предшествует изучению дисциплин:

Проектирование интерактивных систем;

Технология открытых систем.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование следующих общекультурных, общепрофессиональных и профессиональных компетенций:

способность самостоятельно и (или) в составе исследовательской группы разрабатывать, исследовать и применять математические модели для качественного и количественного описания явлений и процессов и (или) разработки новых технических средств (ПК-1);

способность применять методы планирования и проведения исследований и экспериментов при выполнении проектов и заданий в избранной предметной области (ПК-9);

владение приемами и методами работы с персоналом, методами оценки качества и результативности труда, способностью оценивать затраты и результаты деятельности научно-производственного коллектива (ПК-10).

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 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	Виды учебных занятий, включая самостоятельную работу				
		Лекции	Практичес-кие и семинарские занятия	Лаборат. работы	Задания, курсовые 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	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»?

1. 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. Стандартизующие документы и организации.

4. Оценка и управление рисков.

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

11. 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 основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

Основная литература

1. Common Criteria for Information Technology Security Evaluation. Introduction and Overview. 1999.
2. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. 1999.
3. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. 1999.
4. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. 1999.
5. Cryptography and Network Security – Principles and Practice by W. Stallings, Prentice-Hall, Englewood Cliffs, New Jersey, 1998

Дополнительная литература

1. Martin Murhammer, Tim Bourne, Tamas Gaidosch, Charles Kunzinger, Laura Rademacher, Andreas Weinfurter. A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions. IBM Red Book. International Technical Support Organization. 1998.
2. Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander Schmid. A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management. IBM Red Book. International Technical Support Organization. 1999.
3. Security in Open Systems by Rob Bagwill, John Barkley (editor), NIST Special Publication, 1994.
4. Интернет. Протоколы безопасности. – М.: Питер, 2001.
5. Роберта Брагг. Система безопасности Windows 2000. – М.: Вильямс, 2001.
11. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети. Анализ технологий и синтез решений. М. ДМК Пресс. 2004.
6. Голдовский И.Безопасность платежей в Интернете.С.-П.Питер. 2001.
7. Мак-Клар С., Скембрей Дж., Курц Дж. Секреты хакеров. Безопасность сетей - готовые решения. М.: Вильямс. 2004.
8. Брэгг Р., Родс-Оусли М., Страссберг К. Безопасность сетей. Полное руководство. М.: Эком. 2006.

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/l-grid2.php.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень 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

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 напрактических занятиях и в качестве курсового задания,

– подготовку к практическим занятиям, 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.

10. Фонд оценочных средств для проведения промежуточной аттестации по итогам обучения

Приложение

ПРИЛОЖЕНИЕ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

по направлению: Прикладные математика и физика (магистратура)
профиль подготовки: Математические и информационные технологии
Факультет управления и прикладной математики
кафедра информатики и вычислительной математи
курс: 1
квалификация: магистр

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

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

1. Компетенции, формируемые в процессе изучения дисциплины

Освоение дисциплины направлено на формирование у обучающегося следующих общекультурных (ОК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

способность самостоятельно и (или) в составе исследовательской группы разрабатывать, исследовать и применять математические модели для качественного и количественного описания явлений и процессов и (или) разработки новых технических средств (ПК-1);

способность применять методы планирования и проведения исследований и экспериментов при выполнении проектов и заданий в избранной предметной области (ПК-9);

владение приемами и методами работы с персоналом, методами оценки качества и результативности труда, способностью оценивать затраты и результаты деятельности научно-производственного коллектива (ПК-10).

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 контрольных заданий, используемых для оценки знаний, умений, навыков

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 стандартизующих 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.

4. 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 так же ни на один наводящий вопрос.

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

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

Зачет проводится по итогам текущей активности в ходе занятий, защиты инициативной курсовой работы, и путем организации специального опроса, проводимого в простой устной форме, в виде беседы преподавателя и студента