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: Информационная безопасность
по направлению:
профиль подготовки:

кафедра информатики и вычислительной математики
курс: 1
квалификация:

Семестры, формы промежуточной аттестации:
1(Осенний) - Дифференцированный зачет
2(Весенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:
лекции: 0 час.
практические и семинарские занятия: 0 час.
лабораторные занятия: 60 час.

Самостоятельная работа: 12 час.

Всего часов: 72, всего зач. ед.: 2

Количество курсовых работ, заданий: 2

Программу составил: Д.А. Подлесных, старший преподаватель

Программа обсуждена на заседании кафедры

30 августа 2016 г.

СОГЛАСОВАНО:

Заведующий кафедрой И.Б. Петров

Начальник учебного управления И.Р. Гарайшина

1. Цели и задачи

Цель дисциплины

изучение понятий информационной безопасности, методов атак на информационные системы и и защиты от них.

Задачи дисциплины

- освоение обучающимися базовых знаний в области информационной безопасности;
- приобретение практических знаний в области защиты информационных систем.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к вариативной части ООП.

Дисциплина «Информационная безопасность» базируется на дисциплинах:

Высшая математика;

Информатика.

Дисциплина «Информационная безопасность» предшествует изучению дисциплин:

Научно-исследовательская работа.

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 планировать и проводить научные эксперименты (в избранной предметной области) и (или) теоретические (аналитические и имитационные) исследования (ПК-1);

способность анализировать полученные в ходе научно-исследовательской работы данные и делать научные выводы (заключения) (ПК-2);

способность использовать основы философских знаний для формирования мировозренченской позиции (ОК-1);

способность анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции (ОК-2).

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:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в лаборатории и сети Интернет;
- культурой постановки и моделирования задач информатики;
- практикой исследования и решения теоретических и прикладных задач;
- навыками теоретического анализа реальных задач, связанных со структурами данных;

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	Виды атак на информационные системы			8		2
2	Способы защиты информации			6		
3	Требования к средствам защиты			4		
4	Проектирование информационных систем в защищенном исполнении			6		
5	Сертификация программных продуктов			2		4
6	Основные положения и методика информационной защиты.			4		
7	Организация и управление информационной безопасностью.			4		4
8	Оценка и управление рисков.			4		2
9	Типы требований информационной безопасности.			4		
10	Введение в криптографические методы.			6		
11	Сетевая безопасность.			6		
12	Безопасность сервисов управления данными.			6		
Итого часов				60		12
Подготовка к экзамену		0 час.				
Общая трудоёмкость		72 час., 2 зач.ед.				

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

Семестр: 1 (Осенний)

1. Виды атак на информационные системы

Сетевые вторжения. Атаки с использованием Интернет. Вредоносные программы – вирусы, троянцы. Атаки типа «отказ в обслуживании». Несанкционированный доступ к данным.

2. Способы защиты информации

Основные понятия криптографии: симметричные и несимметричные алгоритмы шифрования, вычисление хэш-значений, электронно-цифровая подпись (ЭЦП). Использование готовыхкриптосредств: Криптопро, Верба, CryptoAPI и криптопровайдеры. Классификация способов защиты информации: организационные, инженерно-технические (межсетевые экраны, замки, шифраторы), программные. Средства безопасности, встроенные в Windows. Модели разграничения доступа: дискреционная, ролевая и мандатная. Системы обнаружения вторжений. СЗИ прикладных ИС: идентификация и аутентификация; реакция на события в системе (протоколирование, оповещения, блокировки); разграничение доступа; контроль целостности данных и ПО;

3. Требования к средствам защиты

Патерн проектирования MVC(Model-View-Controller). MVC в Cocoa. Работа нескольких MVC вместе.

4. Проектирование информационных систем в защищенном исполнении

Этапы работы над системой: обследование, подготовка Техзадания, эскизное проектирование, техническое проектирование, разработка, документирование, тестирование, опытная эксплуатация, промышленная эксплуатация. Формулирование политики безопасности. Задание по безопасности и профиль безопасности. Взаимодействие средств защиты информационной системы, базы данных и операционной системы. Понятие доверенной системы. Особенности архитектуры и программно-технической реализации: выделение Диспетчера доступа, использование идентификации Windows, применяемые сетевые

5. Сертификация программных продуктов

Общие сведения о системе сертификации информационных систем и средств вычислительной техники в РФ: цель сертификации, нормативные документы, выполняемые проверки.

6. 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.

Семестр: 2 (Весенний)

7. Организация и управление информационной безопасностью.

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

8. Оценка и управление рисков.

Оценка и управление рисков. Оценка и управление рисков. Уязвимости и оценка потенциальных потерь.

9. Типы требований информационной безопасности.

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

10. Введение в криптографические методы.

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

11. 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.

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)

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

Для контроля и коррекции знаний обучающиеся могут использовать компьютерное тестирование, в том числе на портале judge.mipt.ru.

8. 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 лабораторным 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 лабораторные занятия.

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

Приложение

ПРИЛОЖЕНИЕ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

по направлению:
профиль подготовки:

кафедра информатики и вычислительной математи

курс: 1
квалификация:

Семестры, формы промежуточной аттестации:

1(Осенний) - Дифференцированный зачет
2(Весенний) - Дифференцированный зачет

Разработчик: Д.А. Подлесных, старший преподаватель

1. Компетенции, формируемые в процессе изучения дисциплины

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

способность планировать и проводить научные эксперименты (в избранной предметной области) и (или) теоретические (аналитические и имитационные) исследования (ПК-1);
способность анализировать полученные в ходе научно-исследовательской работы данные и делать научные выводы (заключения) (ПК-2);
способность использовать основы философских знаний для формирования мировозренченской позиции (ОК-1);
способность анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции (ОК-2).

2. Показатели оценивания компетенций

В результате изучения дисциплины «Информационная безопасность» 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:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в лаборатории и сети Интернет;
- культурой постановки и моделирования задач информатики;
- практикой исследования и решения теоретических и прикладных задач;
- навыками теоретического анализа реальных задач, связанных со структурами данных;

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