Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Рабочая программа дисциплины

Защита информации в корпоративных сетях

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

В курсе содержится информация о межсетевых экранах (установка и использование), сведения о безопасности беспроводных соединений и настольных компьютеров, о биометрических методах аутентификации и других современных способах защиты.

Рассказывается о видах компьютерных атак и о том, как они воздействуют на организацию; приводятся сведения о базовых службах безопасности, используемых для защиты информации и систем.

Рассматриваются вопросы разработки полноценной программы и политики безопасности, современного состояния законодательных норм в области информационной безопасности, управления рисками и системой безопасности.

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Задачи освоения дисциплины

2.1. Вводятся общие понятия информационной безопасности, рассматривается история развития этого понятия. Анализируются современные стандарты обеспечения информационной безопасности. Определяются основные компоненты защиты информации. Рассматриваются различные категории атак и хакерские методы взлома. Формулируются рекомендации по организации работы службы безопасности на предприятии. Анализируются средства технической безопасности. Рассматриваются плюсы и минусы их использования. Рассматриваются современные беспроводные технологии и вопросы их безопасности.

2.2. Рассматриваются вопросы политики информационной безопасности, методики разработки политик, создания, развертывания и эффективного использования. Также рассмотрены вопросы обеспечения информационной безопасности, оценки стоимости проведения мероприятий по безопасности. Уделено внимание вопросам разработки и реализации политики безопасности, а также аудита систем.

2.3. Рассмотрены различные механизмы, обеспечивающие информационную безопасность, такие как межсетевые экраны и их различные архитектуры, методы различные методы шифрования (с закрытым и открытым ключом) и др.

Знать – 2.1; уметь – 2.2, владеть – 2.3.

Для достижения поставленной цели и решения заявленных задач используются традиционное обучение и современные образовательные технологии: ИКТ (в т.ч. LMS iDO, цифровые инструменты из п. 13), групповая работа, игровые методы обучения, технология развития критического мышления, развивающее обучение, разноуровневое обучение.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в модуль «Специализация».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Четвертый семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Ведение в компьютерную безопасность» и «Организационное и правовое обеспечение информационной безопасности».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-лабораторные: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

На аудиторные занятия лекционного типа отводится 32 часа (10 тем по 2 часа, 3 темы по 4 часа). По некоторым темам предусмотрены лабораторные работы, всего 16 часов (4 лабораторные работы по 4 часа).

Самостоятельная работа обучающихся является наиболее продуктивной формой образовательной и познавательной деятельности; направлена на углубление и закрепление знаний, развитие практических умений и включает в себя работу с лекционным материалом, подготовку к текущей и промежуточной аттестации.

Тема 1. Основные термины и понятия информационной безопасности.

Вводится общее понятие информационной безопасности, рассматривается краткая история ее развития. Анализируются современные стандарты обеспечения информационной безопасности. Определяются основные компоненты защиты информации.

Тема 2. Основные категории атак.

В данной теме рассмотрены различные категории атак, даны их определения и условия для их осуществления. Коротко рассмотрен механизм проведения атак.

Тема 3. Методы хакеров

Данная тема посвящена хакерским атакам. Рассмотрена мотивация деятельности хакеров, история методов взлома, различные способы проведения атак. Рассмотрены виды вредоносного ПО, а также способы выявления хакерских атак различных типов.

Тема 4. Службы информационной безопасности

Рассмотрены основные службы безопасности, проблемы конфиденциальности информации, ее целостности и доступности в компьютерных системах.

Тема 5. Политика.

Рассмотрены вопросы политики информационной безопасности, методика разработки политик, создания, развертывания и эффективного использования.

Тема 6. Управление риском.

Дано определение риска. Уделено внимание вопросам выявления возможных рисков. Рассмотрен вопрос оценки возможных рисков.

Тема 7. Обеспечение информационной безопасности.

Рассмотрены вопросы обеспечения информационной безопасности, оценки стоимости проведения мероприятий по безопасности. Уделено внимание вопросам разработки и реализации политики безопасности, а также аудита систем.

Тема 8. Рекомендации по обеспечению сетевой безопасности.

Вводится понятие административной безопасности. Даются рекомендации по организации работы службы безопасности на предприятии. Анализируются средства технической безопасности. Рассматриваются плюсы и минусы использования стандарта ISO 17799.

Тема 9. Межсетевые экраны.

В лекции рассмотрены различные типы межсетевых экранов и их различные архитектуры.

Тема 10. Виртуальные частные сети.

Рассмотрены вопросы, связанные с VPN. Дано их определение. Рассмотрены два типа VPN, их преимущества и недостатки. Дано понятие стандартных технологий функционирования VPN.

Тема 112. Шифрование.

Рассмотрены основные концепции шифрования, различные виды шифрования (с закрытым и открытым ключом), вопросы управления ключами. Дано понятие цифровой подписи. Уделено внимание вопросам доверия в информационных системах.

Тема 12. Обнаружение вторжений.

Лекция посвящена вопросам обнаружения вторжений. Рассмотрены основные типы систем обнаружения вторжений и датчиков вторжений. Уделено внимание вопросам установки, управления IDS и предотвращения вторжений посредством их.

Тема 13. Безопасность беспроводных соединений.

Лекция посвящена безопасности беспроводных сетей. Рассмотрены современные беспроводные технологии, вопросы безопасности беспроводных сетей.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения лабораторных работ, проведения тестирования по лекционному материалу, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Выполнение лабораторной работы оценивается в 2 балла:

0 баллов. Студент слабо разбирается или не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

1 балл. Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы, возможно, с негрубыми ошибками. Представляет работу на защите удовлетворительно.

2 балла. Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в четвертом семестре проводится в письменной форме. Экзаменационное задание состоит из трех теоретических вопросов. Продолжительность экзамена 1,5 часа.

Теоретические вопросы и лабораторные задания проверяют ИПК-2.1, ИПК-2.2, ИПК-2.3. Ответ на вопрос дается в развернутой форме.

Примеры теоретических вопросов:

1. Что такое информационная безопасность?

2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню С2 правительства США, самыми защищенными?
6. Почему безопасность – это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню А1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню С2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Ответ на каждую часть экзаменационного задания оценивается по системе от 0 до 3 баллов. Экзамен считается состоявшимся, если в ходе экзамена студент набрал от 4 до 9 баллов. Экзаменационная оценка определяется суммой баллов, набранных студентом в течение семестра и в ходе экзамена.

Критерии оценки ответа на теоретический вопрос:

3 балла: полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; специальные термины используются правильно; определения приведены верно; допущены одна–две неточности при освещении вопросов, которые исправляются по замечанию преподавателя.

2 балла: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; в изложении допущены небольшие пробелы, не исказившие содержание ответа, или допущены один–два недочета при освещении содержания ответа, исправленные по замечанию преподавателя.

1 балл: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов.

0 баллов: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей, или наиболее важной части вопроса; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.

Оцениваемая работа обучающегося по курсу разделена на четыре блока: 1) комплексная контрольная точка в середине семестра; 2) прохождение тестов по материалам лекций в течение семестра; 3) выполнение лабораторных работ; 4) экзаменационное задание.

Баллы по Блоку 1 формируются суммированием баллов за каждую часть в рамках комплексной контрольной точки: 1) ответ на два теоретических вопроса (критерии оценивания ответа на теоретический вопрос приведены выше); 2) выполнение первых двух лабораторных работ; 3) групповая работа (групповая работа оценивается по системе от

0 до 3, критерии оценивания групповой работы доводятся до обучающихся в момент выдачи задания).

Баллы по Блоку 2 формируются суммированием баллов за каждый тест (1 балл – тест пройден: 0 баллов – тест не пройден). Всего 13 тестов (по количеству лекционных тем).

Баллы по Блоку 3 формируются суммированием баллов за выполнение каждой лабораторной работы (всего четыре).

Баллы по Блоку 4 формируются суммированием баллов за каждое экзаменационное задание (критерии оценивания ответа на теоретический вопрос приведены выше).

В таблице 1 приведена шкала оценивания каждого блока, а в таблице 2 – шкала формирования оценки за курс.

Таблица 1 – Оценивание каждого из трех блоков работы обучающегося по курсу

Оценка за блок	Количество баллов			
	Блок 1	Блок 2	Блок 3	Блок 4
«отлично»	7–9	11–13	6–8	8–9
«хорошо»	5–6	8–10	6–5	6–8
«удовлетворительно»	3–4	6–7	3–5	4–5
«неудовлетворительно»	0–2	0–5	0–2	0–3

Таблица 2 – Условия формирования оценки за курс

Оценка за курс	Условие формирования оценки за курс
«отлично»	За все блоки «отлично» Один или два блока «хорошо» остальные «отлично»
«хорошо»	Один блок «отлично» остальные «хорошо» За все блоки «хорошо» Один блок «удовлетворительно» остальные «хорошо» или «отлично»
«удовлетворительно»	Один блок «неудовлетворительно» остальные «хорошо» или «отлично» Все блоки «удовлетворительно» Да блока «удовлетворительно» остальные «хорошо» или «отлично»
«неудовлетворительно»	Все остальные случаи

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO.

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2008. – 225 с.

– Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.

– Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

– Макаренко С. И. Защита компьютерных сетей и телекоммуникаций. Учебное пособие. – СПб.: Наукоемкие технологии, 2024. – 311 с.

– Воробьев С. П. Компьютерные сети и сетевая безопасность: учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск: ЮРГПУ (НПИ), 2022. — 216 с.

– Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание – СПб.: Питер, 2021. – 1008 с.

б) дополнительная литература:

– Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с.

в) ресурсы сети Интернет:

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.