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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 16 » ноября 2023 г.

Рабочая программа дисциплины

Основы информационной безопасности

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.03.01

СОГЛАСОВАНО:
Руководитель ОП
_____ В.Н. Тренькаев

Председатель УМК
_____ С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-1 – Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– ОПК-8 – Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

– ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем.

– ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности.

ИОПК-1.2 Понимает значение информации, информационных технологий и информационной безопасности в развитии современного общества.

ИОПК-1.3 Выявляет влияние информации, информационных технологий и информационной безопасности на объективные потребности личности, общества и государства.

ИОПК-8.1 Осуществляет подбор, изучение и обобщение научно-технической информации, методической информации отечественного и зарубежного опыта по проблемам компьютерной безопасности.

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации.

2. Задачи освоения дисциплины

– Формирование представлений о базовых понятиях и задачах, средствах и методах информационной безопасности, государственной политике РФ в сфере информационной безопасности, особенностях обеспечения информационной безопасности в компьютерных сетях и системах.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Общие вопросы компьютерной безопасности".

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

Второй семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: Информатика, Архитектура вычислительных систем, Дискретная математика.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е., 72 часа, из которых:
-лекции: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Информация как объект защиты.
Понятие об информации. Уровни представления информации.
Свойства защищаемой информации. Виды тайн.
Правовой режим информационных ресурсов.

Тема 2. Понятийный аппарат информационной безопасности.
Виды, способы, замысел, объект, техника защиты информации.
Виды нарушителя и классификация угроз.

Тема 3. Государственная политика информационной безопасности.
Государственная система обеспечения информационной безопасности.
Законодательная основа обеспечения информационной безопасности.
Безопасность критической информационной инфраструктуры РФ.
Доктрина информационной безопасности РФ. ФСТЭК.

Тема 4. Угрозы безопасности информации.
Несанкционированные операции с информацией. Перечень типовых угроз.
Классификация уязвимостей и угроз. Классификация способов НСД.
Типовые атаки на коммуникационные протоколы.
Международные базы данных и реестры уязвимостей.
Банк данных угроз безопасности информации ФСТЭК России.

Тема 5. Меры противодействия угрозам безопасности.
Правовое обеспечение информационной безопасности.
Организационные, физические, технические меры.
Политика информационной безопасности организации.

Тема 6. Криптографические методы защиты информации.
Основные задачи криптографии. Криптографические системы.
Криптографические протоколы. Цифровая подпись. Хеш-функция.
Стандарты в области криптографической защиты информации.

Тема 7. Основные механизмы защиты от несанкционированного доступа.
Контроль целостности. Идентификация. Протоколирование и аудит.
Управление доступом. Защита от вредоносных программ.
Защита межсетевого взаимодействия. Защита информации при передаче.
Предотвращение утечек информации.

Тема 8. Информационная безопасность компьютерных сетей.
Угрозы корпоративной сети. Защита периметра. Основные механизмы защиты.

Базовые средства защиты компьютерных сетей: межсетевые экраны, системы анализа защищенности, системы обнаружения атак. Виртуальные частные сети (VPN). Аудит безопасности.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, выполнения контрольных заданий и фиксируется в форме контрольной точки не менее одного раза в семестр.

Типовые контрольные задания для проведения текущего контроля успеваемости по дисциплине.

Тема “Понятийный аппарат информационной безопасности”. Задание. Используя Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), требуется детально изучить три угрозы безопасности информации (описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы), присущих некоторому одному выбранному студентом объекту (облачная система, грид-система, BIOS, виртуальная машина, беспроводная сеть, web-приложение, хранилище больших данных и т.п.), а также три устраненные уязвимости для некоторого одного выбранного студентом ПО (СУБД MySQL, Браузер Google Chrome и т.п.). Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение основными понятиями информационной безопасности. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы: 1) список определений терминов: угроза, уязвимость, конфиденциальность, целостность, доступность; 2) список изученных угроз и уязвимостей.

Тема “Информационная безопасность компьютерных сетей”. Задание. Требуется выбрать какое-либо программное средство защиты информации (СЗИ) от какого-либо производителя, изучить предназначение системы/средства/инструмента: какие задачи решаются и какие методы/подходы/алгоритмы используются для решения данных задач, архитектуру (схему работы), функциональные возможности и характеристики средства. Излученный материал излагается в виде краткого реферата с указанием источников информации. После чего надо скачать, установить пробную версию изученного СЗИ, и настроить, активизируя базовые возможности продукта. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы в виде реферата и скриншотов (снимков экрана) с настройками СЗИ. Примеры СЗИ: КриптоПро CSP – криптопровайдер, Secret Net Studio - защита конечных точек, Kaspersky Small Office Security - защита для малого бизнеса.

Тема “Криптографические методы защиты информации”. Задание “Шифры замены и перестановки”. Требуется зашифровать свое ФИО: 1) лозунговым шифром; 2) шифром Виженера; 3) шифром вертикальной перестановки; расшифровать произвольное слово из предложенного списка и зашифрованное шифром Виженера при известном ключе. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название

дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы.

Тема “Основные механизмы защиты от несанкционированного доступа”. Задание “Руководящие документы”. Используя сайт ФСТЭК России (Федеральная служба по техническому и экспортному контролю) http://fstec.ru/, выбрать СЗИ в Государственном реестре сертифицированных средств защиты информации, которое имеет сертификат на соответствие одному или нескольким руководящим документам: либо по уровню контроля отсутствия НДВ (недекларированных возможностей), либо по классу защищенности СВТ (средств вычислительной техники), либо по классу защищенности МЭ (межсетевых экранов), либо по классу защищенности АС (автоматизированных систем), изучить соответствующий(ие) руководящий(ие) документ(ы), описать требования, которые предъявляются к выбранному средству защиты с точки зрения соответствия классу защищенности выбранного СЗИ. Студент должен самостоятельно выполнить задание, выложить отчет в систему управления обучением Moodle, при необходимости продемонстрировать преподавателю при устной защите владение материалом. Отчет включает в себя: название дисциплины и задания, ФИО и номер группы исполнителя работы, результат выполнения работы.

Выполнение заданий оценивается по бинарной системе (зачет/незачет): зачет - студент в целом удовлетворительно разбирается в задаче, хорошо знает материал, отвечает на вопросы с замечаниями или с негрубыми ошибками; незачет - студент слабо разбирается в задаче, плохо знает материал, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя. Допуском до зачета является выполнение 80% заданий.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Промежуточная аттестация осуществляется на основе проверки выполнения контрольных заданий и/или по результатам собеседования с использованием перечня контрольных вопросов по курсу. Схема вопросов зачета должна соответствовать компетентностной структуре дисциплины. При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов – результатов обучения.

Примерный перечень вопросов к зачету:

1. Уровни представления информации.
2. Свойства защищаемой информации.
3. Виды тайн (государственная, служебная, профессиональная и др.).
4. Термины, относящиеся к видам защиты информации.
5. Термины, относящиеся к способам защиты информации.
6. Термины, относящиеся к замыслу защиты информации.
7. Термины, относящиеся к объекту защиты информации.
8. Термины, относящиеся к угрозам безопасности информации.
9. Термины, относящиеся к технике защиты информации.
10. Национальная безопасность РФ.
11. Доктрина информационной безопасности РФ.
12. Законодательная основа обеспечения информационной безопасности.
13. Нормативная основа обеспечения информационной безопасности.

14. Безопасность критической информационной инфраструктуры РФ.
15. Государственная система обеспечения информационной безопасности.
16. Несанкционированные операции с информацией.
17. Источники и классификация угроз.
18. Перечень типовых непреднамеренных искусственных угроз.
19. Перечень типовых преднамеренных искусственных угроз.
20. Классификация способов несанкционированного доступа.
21. Типовые атаки на коммуникационные протоколы.
22. Законодательные меры противодействия угрозам безопасности.
23. Организационные меры противодействия угрозам безопасности.
24. Физические и технические меры противодействия угрозам безопасности.
25. Аутентификация. Невозможность отказа от авторства.
26. Имитозащита. Цифровая подпись.
27. Симметричный / асимметричный шифр.
28. Криптографическая стойкость шифра.
29. Метод криптографического анализа.
30. Криптографический протокол.
31. Криптографическая хеш-функция.
32. Классификация криптопротоколов.
33. Свойства цифровой подписи.
34. Криптографические протоколы аутентификации сообщений.
35. Криптографические протоколы идентификации.
36. Объект, субъект, доступ к информации, правила разграничения доступа.
37. Идентификация, аутентификация, авторизация.
38. Протоколирование и аудит (активный аудит).
39. Статистический метод обнаружения атак.
40. Сигнатурный метод обнаружения атак.
41. Дискреционное управление доступом.
42. Мандатное управление доступом.
43. Ролевое управление доступом.
44. Защита информации при хранении и передаче.
45. Защита от вредоносных программ.
46. Виды компьютерных вирусов и вредоносных программ.
47. Защита межсетевого взаимодействия.
48. Предотвращение утечек информации.
49. Аудит безопасности.
50. Угрозы корпоративной сети. Защита периметра сети.
51. Основные механизмы защиты корпоративной сети.
52. Средства защиты информации: межсетевые экраны.
53. Средства защиты информации: виртуальные частные сети.
54. Средства защиты информации: системы анализа защищенности.
55. Средства защиты информации: системы обнаружения атак.
56. Системы предотвращения утечки конфиденциальной информации.
57. Политика информационной безопасности организации.

Критерии оценивания промежуточной аттестации:

Зачет по дисциплине – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства контрольных заданий.

Незачет по дисциплине – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении контрольных заданий.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle»

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

в) Семинарских / практических занятий по дисциплине нет.

г) Лабораторных работ по дисциплине нет.

д) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа со слайдами лекции; изучение вопросов, выносимых за рамки лекционных занятий; выполнение контрольных заданий; подготовка к рубежному контролю по теме/разделу (аттестации). Работу со слайдами (конспектом) лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы. Контрольные задания, приведенные в планах занятий, выполняются студентами в обязательном порядке.

Методические указания обучающимся по освоению дисциплины: целенаправленно, систематически и планомерно работать со слайдами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; тратить не менее часа в день на самостоятельную работу; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе Moodle ТГУ; работать с тематическими форумами в сети Интернет.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Нестеров С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2019. - 324 с.

– Баранова Е.К. Основы информационной безопасности: учебник/ Е.К. Баранова, А.В. Бабаш. - Москва: РИОР : ИНФРА-М, 2019. - 202 с.

– Е.В. Вострецова Основы информационной безопасности : учебное пособие / Е. В. Вострецова. - Екатеринбург : Изд-во Урал. университета, 2019. - 204 с.

б) дополнительная литература:

– Галатенко В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 4-е изд.. - Москва : Интернет-Университет Информационных Технологий, 2010. - 205 с.

– Е.Б. Белов Основы информационной безопасности: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Горячая линия - Телеком, 2006. - 544 с.

– Бондарев, В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. - Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. - 250 с.

в) ресурсы сети Интернет:

– Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/10/10/info

– Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/2259/155/info

– Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/102/102/info

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– ОС Windows/Linux, браузер Firefox/Яндекс

– 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/

в) профессиональные базы данных:

– Банк данных угроз безопасности информации ФСТЭК России- https://bdu.fstec.ru/

– National Vulnerability Database (NVD) - https://nvd.nist.gov/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного 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.

15. Информация о разработчиках

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности