Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Математические методы оценки защищенности компьютерных систем

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов V курса очной формы обучения

Составитель:

к.ф.м.н., доцент _____ Н.А. Семыкина

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Математические методы оценки защищенности компьютерных систем

2. Цель и задачи дисциплины (или модуля)

Целью освоения дисциплины «Математические методы оценки защищенности компьютерных систем» является приобретение студентами знаний о целях и основных методах экспертных оценок и о возможности применения этих методов для решения практических задач в приложении к компьютерной безопасности.

В задачи дисциплины входит: изучить теоретические подходы математических методов, применяемых при моделировании и оценки защищенности компьютерных систем, умение ставить задачи исследования и определять наиболее адекватные математические методы, способствующие решению поставленной задачи.

3. Место дисциплины (или модуля) в структуре ООП

Данная является дисциплиной вариативной части для 2013 – 2016 гг. набора и дисциплиной базовой части для 2017 г. набора. Для успешного изучения данной дисциплины необходимо знание основ следующих дисциплин «Теория вероятностей и математическая статистика», «Модели безопасности компьютерных систем».

4. Объем дисциплины (или модуля):

4 зачетных единиц, 144 академических часа, **в том числе**

контактная работа: лекции 36 часов, практические занятия 36 часов, **самостоятельная работа:** 45 часов, контроль: 27 часов.

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

Планируемые результаты освоения	**Планируемые результаты обучения по дисциплине (или модулю)**

образовательной программы (формируемые компетенции)	
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** навыками использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации. **Уметь:** обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования **Знать:** формальные модели безопасности; методы обоснования требований и оценки защищенности систем обработки информации; порядок сертификации защищенных систем обработки информации.
ПСК 2.3 способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	**Владеть:** методами реализации оценки защищенности компьютерных сетей. **Уметь:** оценивать принимаемые управленческие решения при помощи математического аппарата, использовать математические модели в комплексной оценки системы защиты информации, делать соответствующие выводы и принимать необходимые решения для осуществления защиты компьютерных сетей **Знать:** математические методы, используемые для оценки защищенности компьютерных сетей.

6. Форма промежуточной аттестации

экзамен.

7. Язык преподавания русский**.**

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа (час.) и контроль
		Лекции	Практические (лабораторные) занятия	
1. Общая модель процесса защиты информации. Основные составляющие СЗИ. Направления СЗИ. Этапы построения СЗИ.	5	2	1	2
2. Основные понятия теории нечетких множеств. Операции над нечеткими множествами	19	4	5	10
3. Методы построения функций принадлежности нечетких множеств	12	3	3	6
4. Методы определения важности критериев. Методы экспертных оценок	16	4	4	8
5. Модель комплексной оценки системы защиты информации на основе матрицы знаний	16	4	4	8

6. Выбор способа использования групп экспертов. Формирование экспертной группы. Анализ информации, полученной от экспертов.	12	3	3	6
7. Введение в теорию принятия решений. Классификация постановки задачи теории принятия решений	16	4	4	8
8. Принятие решения в условиях нескольких критериев выбора	16	4	4	8
9. Принятие решения в условиях риска	16	4	4	8
10. Принятие решения в условиях противодействия. Введение в теорию игр	16	4	4	8
ИТОГО	144	36	36	72

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Планы практических (семинарских) занятий и методические рекомендации

РАЗДЕЛ 1. СИСТЕМЫ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ.

Основные составляющие СЗИ. Направления СЗИ. Этапы построения СЗИ. Матрица знаний (оценок). Особенности оценки СЗИ. Модели СЗИ.

РАЗДЕЛ 2. НЕЧЕТКИЕ МНОЖЕСТВА.

Основные понятия теории нечетких множеств. Операции над нечеткими множествами. Свойства нечетких множеств. Нечеткие числа. LR-форма нечетких чисел. Методы построения функций принадлежности нечетких множеств. Нечеткая логика.

РАЗДЕЛ 3. МЕТОДЫ ЭКСПЕРТНЫХ ОЦЕНОК.

Организация опроса коллектива экспертов. Постановка задачи формирования экспертной группы. Методы экспертных оценок. Методы попарных сравнений. Метод Саати. Ранговые и балльные методы оценки. Методы аппроксимации функции полезности. Методы трансформации частот. Оценка частных показателей. Принцип термометра. Оценка качества СЗИ на основе матрицы знаний.

РАЗДЕЛ 4. ТЕОРИЯ ПРИНЯТИЯ РЕШЕНИЙ

Классификация задач теории принятия решений. Постановка задачи критериального анализа**.** Аксиома Парето**.** Методы принятия решений. Принятие решения в условиях нескольких критериев выбора. Принятие решений в условиях конфликта или противодействия. Процесс принятия управленческих решений.

Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа студентов по изучаемой дисциплине призвана, не только, закреплять знания, полученные во время аудиторных занятий, но и способствовать развитию у студентов творческих навыков, инициативы, умению организовывать свое время.

Все виды самостоятельной работы и планируемые на их выполнение затраты времени в часах исходят из того, что студент достаточно активно работал в аудитории, слушая лекции и решая задачи на практических занятиях. В случае пропуска лекций и практических занятий студенту потребуется сверхнормативное время на освоение пропущенного материала.

При выполнении плана самостоятельной работы студенту необходимо прочитать теоретический материал, содержащийся в указанной учебной литературе и Интернет-ресурсах.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

Типовые контрольные задания для проверки уровня сформированности компетенций

<table>
<tr><th>Этап формирования компетенции, в котором участвует дисциплина</th><th>Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)</th><th>Показатели и критерии оценивания компетенции, шкала оценивания</th></tr>
<tr><td>Базовый

Владеть</td><td>1. При работе ПК необходимо периодически приостанавливать обработку информации и проверять ПК на наличие в нем вирусов. Приостановка в обработке информации приводит к определённым экономическим издержкам. В случае же если вирус вовремя обнаружен не будет, возможна потеря и некоторой части информации, что приведёт и ещё к большим убыткам.
Варианты решения таковы: E1– полная проверка; E2– минимальная проверка; E3– отказ от проверки. ПК может находиться в следующих состояниях: F1– вирус отсутствует; F2– вирус есть, но он не успел повредить информацию; F3– есть файлы, нуждающиеся в восстановлении.
Результаты, включающие затраты на поиск вируса и его ликвидацию, а также затраты, связанные с восстановлением информации, имеют вид:
<table><tr><td></td><td>F_1</td><td>F_2</td><td>F_3</td></tr><tr><td>E_1</td><td>-20.0</td><td>-22.0</td><td>-25.0</td></tr><tr><td>E_2</td><td>-14.0</td><td>-23.0</td><td>-31.0</td></tr><tr><td>E_3</td><td>0</td><td>-24.0</td><td>-40.0</td></tr></table>Построить матрицу потерь и определить вариант действий, используя критерий Сэвиджа
2. Рассмотрим игру двух игроков: администратора безопасности и злоумышленника. Графическим методом найти решение игры, заданной матрицей
$A = \begin{pmatrix} -1 & 8 & 7 & 6 & 3 & 1 \\ 9 & 0 & 1 & 2 & 5 & 7 \end{pmatrix}$.</td><td>Имеется полное верное решение, включающее правильный ответ – 5 балла
В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла
Решение не дано или дано неверное решение – 0 баллов</td></tr>
<tr><td>Базовый
Уметь</td><td>1. Была проведена оценка защищенности компьютерной сети в трех подразделениях по пяти факторам. Ниже в таблице приведены результаты оценивания. Привести значения критериев к одинаковым единицам. Используя мультипликативную свёртку, выяснить, какое подразделение защищено лучшим образом. Веса критериев: $\lambda_1 = 0{,}6$; $\lambda_2 = 0{,}7$; $\lambda_3 = 0{,}4$; $\lambda_4 = 0{,}5$; $\lambda_5 = 0{,}8$.
<table><tr><td>факторы
подразделение</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>A</td><td>15 чел.</td><td>50 тыс. руб</td><td>4 шт.</td><td>3 месяца</td><td>- 372 тыс. руб</td></tr><tr><td>B</td><td>17 чел.</td><td>75 тыс. руб</td><td>3 шт.</td><td>2 месяца</td><td>-256 тыс.</td></tr></table></td><td>Имеется полное верное решение, включающее правильный ответ – 5 балла
В решении имеются лишние или неверные записи, не отделенные от решения – 3</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td></td><td></td><td>руб</td></tr>
<tr><td>С</td><td>20 чел.</td><td>70 тыс. руб.</td><td>7 шт.</td><td>1 месяц</td><td>-538 тыс.руб.</td></tr>
</table>
2. Используя матрицу знаний оценить качество системы защиты информации 3 корпуса ТвГУ по направлению Защита каналов связи.
</td><td>балла
Решение не дано или дано неверное решение – 0 баллов</td></tr>
<tr><td>Базовый
Знать</td><td>1. Требуется провести оценку защищенности компьютерной сети по классу средств вычислительной техники (СВТ). Ниже в таблице приведены результаты оценивания значимость каждого критерия балльным методом (10-балльная шкала) двумя экспертами. Выставите свои оценки за 3 эксперта и определите четыре основных критерия. Найдите весовые коэффициенты важности этих критериев.
<table>
<tr><td>Показатель защищенности по классу средств вычислительной техники</td><td>1 эксперт</td><td>2 эксперт</td><td>3 эксперт</td></tr>
<tr><td>1 очистка памяти</td><td>8</td><td>7</td><td></td></tr>
<tr><td>2 регистрация</td><td>9</td><td>5</td><td></td></tr>
<tr><td>3 идентификация и аутентификация</td><td>9</td><td>10</td><td></td></tr>
<tr><td>4 взаимодействие пользователя с комплексом средств защиты</td><td>7</td><td>10</td><td></td></tr>
<tr><td>5 руководство по комплексу средств защиты</td><td>10</td><td>9</td><td></td></tr>
<tr><td>6 защита ввода вывода на отчуждаемый физический носитель информации</td><td>5</td><td>4</td><td></td></tr>
</table>
2. Для оценки защищенности по классу СВТ было предложено три объекта:
1) Третий корпус Тверского госуниверситета, аудитория 16.
2) Организация, в которой Вы проходили летнюю практику.
3) Расчетная группа Тверского госуниверситета, ректорат, 14 кабинет.
Какой из трех объектов имеет более высокий уровень защиты по классу СВТ? Определить</td><td>Имеется полное верное решение, включающее правильный ответ – 5 балла
В решении имеются лишние или неверные записи, не отделенные от решения – 3 балла
Решение не дано или дано неверное решение – 0 баллов</td></tr>
</table>

	ранговым методом.	

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература

Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях : [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – Часть 1. – 171 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612167 ,

Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644

б) Дополнительная литература:

Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

SecurityLab.ru
Независимый информационно-аналитический портал по безопасности
SASecurity Information Box

Информационная безопасность на Report.ru
Информационная безопасность / Блог / Хабрахабр
Библиотека информационной безопасности
Библиотека сетевой безопасности
Компьютерная безопасность: уязвимости, ошибки и эксплоиты
Построение безопасности в сетях
openPGP в России

VII. Методические указания для обучающихся по освоению дисциплины

Требования к рейтинг-контролю.

Модули.	Темы.	Виды контроля.	Максимальное количество баллов.	Формы контрольных испытаний.
Модуль I.	Темы раздела 1 – 2.	Текущий.	15	1) контроль посещения занятий, 2) устный опрос, 3) контроль за выполнением индивидуальных заданий.
		Рубежный.	15	контрольная работа.
Модуль II.	Темы раздела 3 – 4	Текущий.	15	1) контроль посещения занятий, 2) устный опрос, 3) контроль за выполнением индивидуальных заданий.
		Рубежный.	15	контрольная работа.
		Итоговый контроль (экзамен).	40	1) ответ по билету, 2) контрольное задание.

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

1) лекционные занятия в аудитории, с использованием мультимедийной установки;
2) практические занятия с использованием средств мультимедиа;
3) **Программное обеспечение**

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски.. Класс ПЭВМ

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№ п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			