Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Экономика защиты информации и управление рисками

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Бойкова А. В.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы знаний об экономической безопасности государства и отдельных организаций, об основных экономических проблемах защиты информации и изучение студентами видов, практических методов и средств проведения аудита информационной безопасности.

Задачами освоения дисциплины являются:

1) ознакомление с основными стандартами в области аудита ИБ, практическими приемами проведения аудита, методами сбора данных, оценки рисков и анализа защищенности;

2) формирование понимания процессов проверки и оценки ИБ, принципов организации процессов аудита и анализа рисков ИБ и подготовки отчетных документов;

3) изучение теоретических и методологических основ моделирования и управления рисками систем и процессов.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в вариативную часть учебного плана и является дисциплиной по выбору, связана с другими дисциплинами образовательной программы: «Экономика», «Инновационная экономика и технологическое предпринимательство».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Сертификация по требованиям безопасности и аттестация объектов информатизации», «Основы управленческой деятельности», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 4 зачетные единицы, 144 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 34 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 49 ч., контроль – 27 ч.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	**УК-9.1** Использует основные принципы экономического анализа (принцип альтернативных издержек, ценности денег с учетом фактора времени и т.п.)
	УК-9.2 Использует правовые базы данных и прочие ресурсы для получения информации

	о своих правах и обязанностях, связанных с осуществлением экономической политики государства
ПК-2. Способен разрабатывать и конфигурировать программные и программно-аппаратные средства защиты информации	**ПК-2.1** Разрабатывает технико-коммерческие предложения и участвует в их защите
ПК-4. Способен организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	**ПК-4.1** Организует и контролирует аналитические работы в ИТ-проекте
	ПК-4.2 Управляет процессами разработки и сопровождения требований к системам и управление качеством систем
	ПК-4.3 Разрабатывает стратегии тестирования и управляет процессом тестирования
ПК-5 Способен производить установку, наладку, тестирование и обслуживание программно-аппаратных средств обеспечения информационной безопасности компьютерных систем	**ПК-5.2** Тестирует системы защиты информации автоматизированных систем

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 10 семестре.

6. Язык преподавания русский**.**

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

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	

Раздел 1 Информация как важнейший ресурс экономики. Экономическая эффективность систем защиты информации	72	17	15	2	38
Раздел 2 Аудит, анализ и управление рисками информационной безопасности.	72	17	15	2	38
ИТОГО	144	34	30	4	76

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1 Информация как важнейший ресурс экономики. Экономическая эффективность систем защиты информации	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления.
Раздел 2 Аудит, анализ и управление рисками информационной безопасности.	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (УК-9.1; УК-9.2; ПК-2.1): Выручка оператора информационных ресурсов составляет 900 тыс. ден. ед., переменные затраты – 200 тыс. ден. ед., постоянные затраты – 270 тыс. ден. ед. Необходимо определить запас финансовой

прочности. Оценить на сколько процентов изменится прибыль предприятия, если эксперты оценивают снижения спроса на услуги оператора информационных ресурсов на 15%? Какой процент прибыли удастся сохранить предприятию, если выручка упадет на 40%? Каким должен быть процент снижения выручки, при котором оператор информационных ресурсов полностью лишится прибыли?

Задание 2 (УК-9.1; УК-9.2; ПК-2.1): Определить затраты на создание информационной системы, если время, затраченное на разработку системы, составляет 2,4 месяца, из них 2 месяца разработчик провел за компьютером. Оклад программиста 15000 руб. Среднегодовая норма рабочего времени 1986 часов. Затраты на материалы составляют 73000 руб., из них 65000 руб. потрачено на приобретение ПК и необходимого оборудования, суммарная мощность потребления электроэнергии которых 650 Вт. Цена электроэнергии 2,1 за 1 кВт/час.

Раздел II.

Задание 1 (ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.2): Составить перечень наиболее распространенных угроз информационной безопасности для данной организации. Выполнить анализ угроз и их последствий, определение слабостей в защите; провести оценку рисков, заполнив типичную форму для анализа рисков (таблица).

Типичная форма для анализа рисков

Описание риска	Возможный эффект	Возможная стоимость риска	Вероятность	Приоритет	Меры защиты	Стоимость мер защиты
1	2	3	4	5	6	7

Пояснения к таблице:

1) В графе 1 содержится описание возможного риска, например: непреднамеренные ошибки пользователей – ввод неверных данных о клиентах.

2) В графе 2 описывается возможный результат, к которому может привести реализация риска, например: потеря клиента или штрафные санкции с его стороны.

3) В графе 3 описывается возможный результат в стоимостном выражении, т.е. что потеряет фирма в результате реализации возможного риска, например: 10000 руб. т.е. что потеряет фирма в результате реализации возможного риска, например: 10000 руб. или в виде оценок: 1 – низкая; 2 – средняя; 3 – высокая оценка стоимости последствий реализации риска.

4) В графе 4 задается вероятность осуществления данного риска. Для вероятности приняты следующие значения: высокая – 0,75; средняя – 0,5; низкая – 0,25; малая – 0,05 или в виде оценок: 1 – низкая; 2 – средняя; 3 – высокая оценка вероятности.

5) В графе 5 задается приоритет данного риска, который определяется как произведение вероятности на возможную стоимость риска и на 10-3 , например: 10000*0,25*10-3 = 2,5 или в виде оценки 2*3= 6

6) В графе 6 описываются предлагаемые меры защиты, которые представляют собой реализацию защитных мероприятий трех направлений пункта 6 применительно к вашей фирме, например: строгий контроль вводимых данных, обеспечиваемый программным способом; обучение персонала; ввод штрафных санкций за допущенные ошибки.
7) В графе 7 задается стоимость мер защиты, предлагаемых в графе 6, например, разработка дополнительного модуля контроля вводимых данных – 5000 руб.; обучение персонала на курсах – 30000 руб.

Представление полученных результатов провести с использованием MS Excel.

Задание 2 (ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.2): Имеются данные о потерях, возникающие из-за отказа серверного оборудования. Оценить степень риска возникновения потерь.

потери	Случаи возникновения потерь						
	1	2	3	4	5	6	7
Web-ресурс №1							
Web-ресурс №2							

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: УК-9.1; УК-9.2; ПК-2.1; ПК-4.1; ПК-4.2; ПК-4.3; ПК-5.2

Каждый студент решает индивидуальный тест и отвечает на теоретический вопрос.

Примерные вопросы к экзамену

1. Понятие аудита безопасности
2. Методы анализа данных при аудите ИБ
3. Анализ информационных рисков предприятия
4. Методы оценивания информационных рисков
5. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
6. Гармонизированные критерии Европейских стран
7. Германский стандарт BSI
8. Британский стандарт BS 7799
9. Международный стандарт ISO 17799
10. Международный стандарт ISO 15408 «Общие критерии»
11. Стандарт COBIT
12. Стандарты по безопасности информационных технологий в России
13. Основные понятия ОК
14. Методология оценки безопасности информационных технологий по ОК
15. Оценка уровня доверия функциональной безопасности информационной технологии
16. Обзор классов и семейств ОК

17. Назначение стандарта ISO 17799 для управления информационной безопасностью
18. Практика прохождения аудита и получения сертификата ISO 17799
19. Анализ видов используемых программных продуктов
20. Система CRAMM 21. Система КОНДОР
22. Сетевые сканеры
23. Задачи и содержание работ при проведении аудита ИБ
24. Подготовка предприятия к проведению аудита ИБ
25. Планирование процедуры аудита ИБ
26. Организация и проведение работ по аудиту
27. Алгоритм проведения аудита безопасности предприятия
28. Перечень и систематизация данных, необходимых для проведения аудита ИБ
29. Выработка рекомендаций и подготовка отчетных документов
30. Экономическая оценка обеспечения ИБ
31Информационная безопасность бизнеса.
32. Развитие службы информационной безопасности.
33. Международная практика защиты информации.
34. Модель Symantec LifeCycle Security.
35. Постановка задачи анализа рисков.
36. Модель Gartner Group.
37. Модель Carnegie Mellon University.
38. Различные взгляды на защиту информации.
39. Национальные особенности защиты информации.
40. Особенности отечественных нормативных документов.
41. Учет остаточных рисков.
42. Международный стандарт ISO 17799.
43. Обзор стандарта BS 7799.
44. Развитие стандарта BS 7799 (ISO 17799).
45. Сравнение стандартов ISO 17799 и BSI.
46. Стандарт США NIST 800-30.
47. Алгоритм описания информационной системы.
48. Идентификация угроз и уязвимостей. Организация защиты информации.
49. Ведомственные и корпоративные стандарты управления ИБ.
50. XBSS-спецификации сервисов безопасности X/Open.
51. Стандарт NASA «Безопасность информационных технологий».
52. Концепция управления рисками MITRE.
53. Вопросы анализа рисков и управления ими.
54. Идентификация рисков.
55. Оценивание рисков.
56. Измерение рисков.
57. Выбор допустимого уровня риска.
58. Выбор контрмер и оценка их эффективности.
59. Разработка корпоративной методики анализа рисков.
60. Постановка задачи.

61. Методы оценивания информационных рисков.
62. Табличные методы оценки рисков.
63. Методика анализа рисков Microsoft.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. - (Высшее образование: Магистратура). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=420080

Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. - Книга из коллекции Лань - Информатика. – Режим доступа: https://e.lanbook.com/book/293009

Григорьев В. К. Управление рисками информационных технологий [Электронный ресурс] : учебное пособие / В. К. Григорьев. - Москва : РТУ МИРЭА, 2023. - 97 с. - Книга из коллекции РТУ МИРЭА - Информатика. – Режим доступа : https://e.lanbook.com/book/329000

б) Дополнительная литература:

Жаркова Н.Н. Управление рисками, системный анализ и моделирование: практикум. - Омский государственный аграрный университет имени П.А.Столыпина, 2019. – 96 с.— Режим доступа: https://e.lanbook.com/book/126631

Щербак А. В. Управление рисками в сфере IT : Монография / А. В. Щербак; Академия управления городской средой, градостроительства и печати. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 243 с. - (Научная мысль). - Дополнительное профессиональное образование. - ISBN 978-5-16-017972-8. – Режим доступа: https://znanium.com/catalog/document?id=426180

2) 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

3) Современные профессиональные базы данных и информационные справочные системы

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.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

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

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	30	10	5	15
2	30	10	5	15

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:
https://www.tversu.ru/sveden/files/Pologhenie_o_reytingovoy_sisteme_obucheniya(1).pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики Компьютерный класс 203а 170002, г.Тверь, Садовый пер-к, д. 35.	Столы, стулья, переносной ноутбук, компьютеры	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
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, у*чебная аудитория* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35	Столы, стулья, переносной ноутбук, проектор	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

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей	Описание внесенных изменений	Дата и протокол заседания

	программы дисциплины (или модуля)		**кафедры, утвердившего изменения**
1.	I - VIII	Создание РПД в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
2.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023