МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»
(ТвГТУ)

УТВЕРЖДАЮ
Проректор
по учебной работе
_____ Э.Ю. Майкова
« _____ » _____ 20____ г.

РАБОЧАЯ ПРОГРАММА

дисциплины части, формируемой участниками образовательных отношений
Блока 1 «Дисциплины (модули)»

«Управление информационной безопасностью»

Направление подготовки бакалавров 09.03.03 Прикладная информатика
Направленность (профиль)– Прикладная информатика в экономике
Типы задач профессиональной деятельности: проектный; организационно-управленческий

Форма обучения – очная, заочная

Факультет информационных технологий
Кафедра «Информационные системы»

Тверь 20___

Рабочая программа дисциплины соответствует ОХОП подготовки бакалавров в части требований к результатам обучения по дисциплине и учебному плану.

Разработчик программы: доцент кафедры ИС В.В. Алексеев

Программа рассмотрена и одобрена на заседании кафедры ИС
«____» _____ 20___ г., протокол № ___.

Заведующий кафедрой Б.В. Палюх

Согласовано
Начальник учебно-методического
отдела УМУ Д.А. Барчуков

Начальник отдела
комплектования
зональной научной библиотеки О.Ф. Жмыхова

1. Цели и задачи дисциплины.

Целью изучения дисциплины «Управление информационной безопасностью» изучение основных принципов управления уровнем информационной безопасности защищаемых ресурсов организации.

Задачами дисциплины являются:

- формирование системы знаний по основным методам управления информационной безопасностью;
- овладение навыками применения основных методов управления уровнем информационной безопасности защищаемых ресурсов организации.

2. Место дисциплины в структуре ОП.

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 ОП ВО. Для изучения курса требуются знания дисциплин «Информационная безопасность», «Теория систем и системный анализ», «Информационные системы и технологии».

Приобретенные знания в рамках данной дисциплины необходимы в дальнейшем в курсах, связанных с построением защищенных информационных систем.

3. Планируемые результаты обучения по дисциплине.

3.1. Планируемые результаты обучения по дисциплине.

Компетенция, закрепленная за дисциплиной в ОХОП:

ПК-1. Способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИПК-1.4. Анализирует и выбирает средства обеспечения информационной безопасности; участвует в управлении информационной безопасностью; исследует выбор проектных решений по защите информации по видам обеспечения информационных систем.

Показатели оценивания индикаторов достижения компетенций

Знать:

З1. Основные методы управления информационной безопасностью.

З2. Методы оценки рисков информационной безопасности.

З3. Основные функции систем управления информационной безопасностью.

Уметь:

У1. Анализировать и выбирать средства обеспечения информационной безопасности.

У2. Исследовать выбор проектных решений по защите информации по видам обеспечения информационных систем.

Иметь опыт практической подготовки:

ПП1. Участия в управлении информационной безопасностью.

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных занятий, лабораторных занятий, самостоятельная работа под руководством преподавателя.

4. Трудоемкость дисциплины и виды учебной работы.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 1а. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	**Зачетные единицы**	**Академические часы**
Общая трудоемкость дисциплины	2	72
Аудиторные занятия (всего)		30
В том числе:		
Лекции		15
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		15
Самостоятельная работа обучающихся (всего)		42
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Реферат		не предусмотрен
Другие виды самостоятельной работы: - подготовка к лабораторным работам		22
Текущий контроль успеваемости и промежуточная аттестация (зачет)		20
Практическая подготовка при реализации дисциплины (всего)		15
в том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		15

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 1б. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	**Зачетные единицы**	**Академические часы**
Общая трудоемкость дисциплины	2	72
Аудиторные занятия (всего)		12
В том числе:		
Лекции		4
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		8
Самостоятельная работа обучающихся (всего)		56+4
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Реферат		не предусмотрен

Другие виды самостоятельной работы: - подготовка к лабораторным работам		22
Текущий контроль успеваемости и промежуточная аттестация (зачет)		20
Практическая подготовка при реализации дисциплины (всего)		8
в том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		8

5. Структура и содержание дисциплины.
5.1. Структура дисциплины

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2а. Модули дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практич. занятия	Лаб. работы	Сам. работа
1	Понятие управления информационной безопасностью	20	6		4	10
2	Политика информационной безопасности	24	5		5	14
3	Система управления информационной безопасностью	28	4		6	18
Всего на дисциплину		**72**	15		15	42

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2б. Модули дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практич. занятия	Лаб. работы	Сам. работа
1	Понятие управления информационной безопасностью	20	2		2	16
2	Политика информационной безопасности	24	1		3	20
3	Система управления информационной безопасностью	28	1		3	24
Всего на дисциплину		**72**	4		8	60

5.2. Содержание дисциплины.

МОДУЛЬ 1 «Понятие управления информационной безопасностью»:

Понятие ISM. Управление информационной безопасностью (ИБ) как часть организационного подхода к управлению безопасностью. Методы и стандарты управления информационной безопасностью. Методы оценки рисков информационной безопасности. Обработка информационных рисков. Расчет рисков по угрозе информационной безопасности. Организация управления персоналом в контексте обеспечения информационной безопасности

МОДУЛЬ 2 «Политика информационной безопасности»:

Понятия политики обеспечения информационной безопасности и политики ИБ организации. Модели доверия в политике безопасности. Основные требования к политике безопасности. Принципы политики безопасности. Содержание корпоративной политики информационной безопасности. Содержание частных политик информационной безопасности. Жизненный цикл политики информационной безопасности. Правовые аспекты применения политики безопасности.

МОДУЛЬ 3 «Система управления информационной безопасностью»:

Актуальность управления обеспечением информационной безопасностью организации. Структура систем управления информационной безопасностью. Процессный подход к управлению информационной безопасностью организации. Управление информационной безопасностью информационно-телекоммуникационных систем организации. Методы построения и внедрения систем управления информационной безопасностью. Анализ эффективности систем управления информационной безопасностью.

5.3. Лабораторные работы

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а. Лабораторные работы и их трудоемкость

Модули. **Цели лабораторных занятий**	**Наименование лабораторных занятий**	**Трудоемкость в часах**
Модуль 1 **Цель:** формирование умений оценки рисков информационной безопасности.	Методы оценки рисков информационной безопасности	4
Модуль 2 **Цель:** формирование умений разработки политики безопасности	Построение политики безопасности защищаемого объекта	5

Модуль 3 **Цель:** формирование умений проектирования и разработки системы управления информационной безопасностью	Разработка эскизного проекта системы управления информационной безопасностью	6

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б. Лабораторные работы и их трудоемкость

Модули. **Цели лабораторных занятий**	**Наименование лабораторных занятий**	**Трудоемкость в часах**
Модуль 1 **Цель:** формирование умений оценки рисков информационной безопасности.	Методы оценки рисков информационной безопасности	2
Модуль 2 **Цель:** формирование умений разработки политики безопасности	Построение политики безопасности защищаемого объекта	3
Модуль 3 **Цель:** формирование умений проектирования и разработки системы управления информационной безопасностью	Разработка эскизного проекта системы управления информационной безопасностью	3

5.4. Практические занятия.

Учебным планом практические работы не предусмотрены

6. Самостоятельная работа обучающихся и текущий контроль успеваемости.

6.1. Цели самостоятельной работы

Формирование способностей к самостоятельному познанию и обучению, поиску литературы, обобщению, оформлению и представлению полученных результатов, их критическому анализу, поиску новых и неординарных решений, аргументированному отстаиванию своих предложений, умений подготовки выступлений и ведения дискуссий.

6.2. Организация и содержание самостоятельной работы

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в подготовке к практическим и лабораторным занятиям, к текущему контролю успеваемости, зачету.

В рамках дисциплины выполняется 3 лабораторных работы, которые защищаются устным опросом. Выполнение всех лабораторных работ обязательно.

В случае невыполнения лабораторной работы по уважительной причине студент должен выполнить пропущенные лабораторные занятия в часы, отведенные на консультирование с преподавателем.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература по дисциплине

1. Суворова, Г.М. Информационная безопасность : учебное пособие для вузов / Г.М. Суворова. - Москва : Юрайт, 2021. - (Высшее образование). - ЭБС Юрайт. - Текст : электронный. - ISBN 978-5-534-13960-0. - (ID=139087-0) URL: https://urait.ru/book/informacionnaya-bezopasnost-467370
2. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А.В. Зенков; Зенков А.В. - Москва : Юрайт, 2021. - (Высшее образование). - ЭБС Юрайт. - Текст : электронный. - (ID=140920-0)
3. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие для учреждений ВПО / Мельников, В.П., Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова - М.: Академия, 2012. - 331 с. - (87414-6)

7.2. Дополнительная литература по дисциплине

1. Чернова, Е.В. Информационная безопасность человека : учебное пособие для вузов по гуманитарным направлениям / Е.В. Чернова. - 2-е изд. - Москва : Юрайт, 2020. - (Высшее образование). - ЭБС Юрайт. - Текст : электронный. - ISBN 978-5-534-12774-4. - (ID=135778-0) URL: https://www.biblio-online.ru/book/informacionnaya-bezopasnost-cheloveka-449350
2. Внуков, А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. - 3-е изд. - Москва : Юрайт, 2020. - (Высшее образование). - ЭБС Юрайт. - Текст : электронный. - ISBN 978-5-534-07248-8. - (ID=135647-0) URL: https://www.biblio-online.ru/book/zaschita-informacii-422772
3. Чепурнова, Н.М. Правовые основы информатики : учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика» / Н.М. Чепурнова, Л.Л. Ефимова; Чепурнова, Н.М., Ефимова, Л.Л. - Москва : ЮНИТИ-ДАНА, 2017. - ЭБС IPR BOOKS. - Текст : электронный. - ISBN 978-5-238-02644-2. - (ID=120865-0) URL: http://www.iprbookshop.ru/81535.html
4. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст]: учеб. пособие для вузов - М.: Горячая ли-ния-Телеком, 2011. - 319 с. - (83830-1) (004; Д 25)
5. Фороузан, Б.А. Криптография и безопасность сетей [Текст]: учеб. пособие / пер. с англ. под ред. А.Н. Берлина - М.: Интернет-Университет Информационных Техно-логий ;БИНОМ. Лаборатория знаний, 2010. - 783 с. - (81861-1) (511; Ф 79)
6. Проскурин, В.Г. Защита программ и данных [Текст]: учеб. пособие для вузов по напр. подготовки 090900 "Информационная безопасность" (бакалавр) и спец. "090301 "Компьютерная безопасность, 090303 "Информационная безопасность автоматизированных систем" - М.: Академия, 2011. - 199 с. - (89165-4)

7. Бабаш, А.В. Информационная безопасность. Лабораторный практикум [Текст]: учеб. пособие / Бабаш, А.В., Баранова, Е.К., Мельников, Ю.Н. - М.: КноРус, 2013. - 131 с. - (96781-8)

7.3. Методические материалы

1. Конспект лекций по дисциплине "Информационная безопасность" направления подготовки 09.03.03 Прикладная информатика. Профиль: Экономика : в составе учебно-методического комплекса / Каф. Информационные системы ; разраб. В.В. Алексеев. - Тверь : ТвГТУ, 2017. - (УМК-Л). - Сервер. - Текст : электронный. - (ID=129588-0)
2. Учебно-методический комплекс дисциплины "Информационная безопасность" направления подготовки 09.03.03 Прикладная информатика. Профиль: Экономика / Каф. Информационные системы ; сост. В.В. Алексеев. - 2017. - (УМК). - Текст : электронный. - 0-00. - (ID=117444-1)

URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/{docId}

7.4. Программное обеспечение по дисциплине

Операционная система Microsoft Windows: лицензии № ICM-176609 и № ICM-176613 (Azure Dev Tools for Teaching).

Microsoft Office 2007 Russian Academic: OPEN No Level: лицензия № 41902814.

Microsoft Visual Studio.

7.5. Специализированные базы данных, справочные системы, электронно-библиотечные системы, профессиональные порталы в Интернет

ЭБС и лицензионные ресурсы ТвГТУ размещены:

1. Электронно-библиотечная система ТвГТУ lib.tstu.tver.ru
2. База данных учебно-методических комплексов cdokp.tstu.tver.ru/emc
3. Подсистема расчета и анализа показателей книгообеспеченности учебного процесса, включая книгообеспеченность кафедр и специальностей на период до 2019 года: cdokp.tstu.tver.ru/site2/wsite/ws_supply.asp?p=ws_supply.asp
4. ЭБС «Юрайт» www.biblio-online.ru
5. ЭБС «Лань» e.lanbook.com
6. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
7. ЭБС «IPRbooks» www.iprbookshop.ru
8. НЭБ ELIBRARY.RU elibrarv.ru
9. Гарант и Консультант Плюс

УМК размещен: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/159215

8. Материально-техническое обеспечение дисциплины

Кафедра «Информационные системы» имеет аудитории для проведения лекций, практических и лабораторных занятий по дисциплине; специализированные учебные классы, оснащенные современной компьютерной техникой, необходимым программным обеспечением, электронными учебными пособиями для проведения лабораторных работ и самостоятельной работы.

Для проведения лабораторных работ имеются лаборатории с персональными компьютерами (наличие локальной вычислительной сети необязательно).

9. Оценочные средства для проведения промежуточной аттестации

9.1 Оценочные средства для проведения промежуточной аттестации в форме экзамена

Учебным планом экзамен по дисциплине не предусмотрен.

9.2. Оценочные средства для проведения промежуточной аттестации в форме зачета

1. Вид промежуточной аттестации в форме зачета.

Вид промежуточной аттестации устанавливается преподавателем:

по результатам текущего контроля знаний и умений обучающегося без дополнительных контрольных испытаний;

по результатам выполнения дополнительного итогового контрольного испытания при наличии у студентов задолженностей по текущему контролю.

2. При промежуточной аттестации без выполнения дополнительного итогового контрольного испытания студенту в обязательном порядке описываются критерии проставления зачёта:

«зачтено» - выставляется обучающемуся при условии выполнения им всех контрольных мероприятий: посещение лекций в объеме не менее 80% контактной работы с преподавателем, выполнения и защиты практических работ.

При промежуточной аттестации с выполнением заданий дополнительного итогового контрольного испытания студенту выдается билет с вопросами и задачами.

Число заданий для дополнительного итогового контрольного испытания - 10.

Число вопросов – 3 (2 вопроса для категории «знать» и 1 вопрос для категории «уметь»).

Продолжительность – 60 минут.

3. Шкала оценивания промежуточной аттестации – «зачтено», «не зачтено».

4. Критерии выполнения контрольного испытания и условия проставления зачёта:

для категории «знать» (бинарный критерий):

ниже базового - 0 балл;

базовый уровень – 1 балла;

критерии оценки и ее значение для категории «уметь» (бинарный критерий):

отсутствие умения – 0 балл;

наличие умения – 1 балла.

Критерии итоговой оценки за зачет:

«зачтено» - при сумме баллов 2 или 3;

«не зачтено» - при сумме баллов 0 или 1.

5. Для дополнительного итогового контрольного испытания студенту в обязательном порядке предоставляется:

база заданий, предназначенных для предъявления обучающемуся на дополнительном итоговом контрольном испытании (типовой образец задания приведен в Приложении);

методические материалы, определяющие процедуру проведения дополнительного итогового испытания и проставления зачёта.

6. Задание выполняется письменно и с использованием ЭВМ.

Перечень вопросов дополнительного итогового контрольного испытания:

1. Понятие ISM. Управление информационной безопасностью (ИБ) как часть организационного подхода к управлению безопасностью.

2. Методы и стандарты управления информационной безопасностью.

3. Методы оценки рисков информационной безопасности. Обработка информационных рисков. Расчет рисков по угрозе информационной безопасности.

4.Организация управления персоналом в контексте обеспечения информационной безопасности

5. Понятия политики обеспечения информационной безопасности и политики ИБ организации. Модели доверия в политике безопасности. Основные требования к политике безопасности.

6. Принципы политики безопасности. Содержание корпоративной политики информационной безопасности. Содержание частных политик информационной безопасности.

7. Жизненный цикл политики информационной безопасности.

8. Правовые аспекты применения политики безопасности.

9. Структура систем управления информационной безопасностью. Процессный подход к управлению информационной безопасностью организации.

10. Методы построения и внедрения систем управления информационной безопасностью. Анализ эффективности систем управления информационной безопасностью.

Пользование различными техническими устройствами, кроме ЭВМ компьютерного класса и программным обеспечением, необходимым для решения поставленных задач, не допускается. При желании студента покинуть пределы аудитории во время экзамена экзаменационный билет после его возвращения заменяется.

Преподаватель имеет право после проверки письменных ответов вопросы задавать студенту в устной форме уточняющие вопросы в рамках задания, выданного студенту.

9.3. Оценочные средства для проведения промежуточной аттестации в форме курсовой работы или курсового проекта

Учебным планом курсовая работа (проект) не предусмотрены.

10. Методические рекомендации по организации изучения дисциплины

Студенты перед началом изучения дисциплины ознакомлены с системами кредитных единиц и балльно-рейтинговой оценки, которые должны быть опубликованы и размещены на сайте вуза или кафедры.

Студенты, изучающие дисциплину обеспечиваются электронными изданиями или доступом к ним, учебно-методическим комплексом по дисциплине, включая методические указания к выполнению практических работ и всех видов самостоятельной работы.

11.Внесение изменений и дополнений в рабочую программу дисциплины

Кафедра ежегодно обновляет содержание рабочих программ дисциплин, которые оформляются протоколами. Форма протокола утверждена Положением о структуре, содержании и оформлении рабочих программ дисциплин, по образовательным программ, соответствующих ФГОС ВО с учетом профессиональных стандартов.

Приложение

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»

Направление подготовки бакалавров 09.03.03 Прикладная информатика
Направленность (профиль) – Прикладная информатика в экономике
Кафедра «Информационные системы»
Дисциплина «Управление информационной безопасностью»

ЗАДАНИЕ ДЛЯ ДОПОЛНИТЕЛЬНОГО ИТОГОВОГО КОНТРОЛЬНОГО ИСПЫТАНИЯ №_1__

1. Вопрос для проверки уровня «ЗНАТЬ» – 0 или 1 балл:
Методы и стандарты управления информационной безопасностью.

2. Вопрос для проверки уровня «ЗНАТЬ» – 0 или 1 балл:
Правовые аспекты применения политики безопасности.

1. Задание для проверки уровня «УМЕТЬ» – 0 или 1 балл:
Выбрать средства обеспечения информационной безопасности для персонального компьютера, подключенного к сети интернет .

Критерии итоговой оценки за зачет:
«зачтено» - при сумме баллов 2 или 3;
«не зачтено» - при сумме баллов 0 или 1.

Составитель: к.т.н., доцент каф. ИС _____ В.В. Алексеев

Заведующий кафедрой ИС: д.т.н., профессор _____ Б.В. Палюх