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 обязательной части Блока 1 «Дисциплины (модули)»
«Безопасность информационных технологий и систем»

Направление подготовки бакалавров – 09.03.02. Информационные системы и технологии

Направленность (профиль) - Разработка, внедрение и сопровождение информационных систем

Типы задач профессиональной деятельности: организационно-управленческий; проектный

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 И.В. Мартынов

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 «Безопасность информационных технологий и систем» является изучение теоретических и практических основ обеспечения безопасности информации в современных информационных системах.

Задачами дисциплины являются:

формирование системы знаний и умений по основным положениям теории информационной безопасности информационных систем и основных технологий построения защищенных информационных систем;

овладение навыками применения основных моделей безопасности и построения защищенных информационных систем.

2. Место дисциплины в структуре ОП.

Для освоения используются знания, полученные на дисциплинах: математика, информатика и программирование, теория вероятностей и математическая статистика, теория систем и системный анализ, вычислительные системы, сети и телекоммуникации, информационные системы, базы данных, высокоуровневые методы информатики и программирования, информационные технологии, операционные среды, системы и оболочки, теория экономических информационных систем.

Приобретенные знания в рамках данной дисциплины необходимы в дальнейшем при выполнении проектно-конструкторской деятельности, а также при выполнении проектной части выпускной квалификационной работы.

3. Планируемые результаты обучения по дисциплине.

3.1. Планируемые результаты обучения по дисциплине.

Компетенция, закрепленная за дисциплиной в ОХОП:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИОПК-3.1. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Показатели оценивания индикаторов достижения компетенций

Знать:

З1.1. Сущность и понятие информации, информационной безопасности и характеристику ее составляющих;

З1.2. Место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

З1.3. Основы организационного и правового обеспечения информационной безопасности, основные нормативно-правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;

З1.4. Базовые понятия, теоремы и алгоритмы теории чисел, используемые в криптографии;

З1.5. Основные виды симметричных и асимметричных криптографических алгоритмов;

З1.6. Криптографические стандарты;

З1.7. Основные виды вредоносных программ и средства их диагностики;

З1.8. Понятия политик безопасности;

З1.9. Каналы утечки речевой информации;

З1.10. Побочные электромагнитные излучения и наводки;

З1.11. Основы законодательства Российской Федерации в области крип защиты информации.

Уметь:

У1.1. Осуществлять поиск и сбор необходимой информации.

У1.2. Проводить сравнительный анализ и выбор средств обеспечения информационной безопасности.

У1.3. Решать стандартные задачи разработки и эксплуатации информационных систем с учетом основных требований информационной безопасности.

У1.4. Формализовать поставленную задачу;

У1.5. Проводить оценку сложности алгоритмов;

ИОПК-3.2. Готовит обзоры, аннотации, составляет рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Знать:

З2. Способы анализа и выбора методов и средств обеспечения информационной безопасности.

Уметь:

У2.1 Применять требования информационной безопасности в профессиональной деятельности.

У2.2 Обосновывать организационно-технические мероприятий по защите информации в ИС.

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных занятий, лабораторных занятий, практических занятий; выполнение курсовой работы.

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	5	180
Аудиторные занятия (всего)		75
В том числе:		
Лекции		30
Практические занятия (ПЗ)		15
Лабораторные работы (ЛР)		30
Самостоятельная работа обучающихся (всего)		69+36 (экз.)
В том числе:		
Курсовая работа		20
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Другие виды самостоятельной работы: - подготовка к лабораторным работам		29
Другие виды самостоятельной работы: - подготовка к практическим работам		20
Текущий контроль успеваемости и промежуточная аттестация (зачет)		не предусмотрен
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		36 (экз.)
Практическая подготовка при реализации дисциплины (всего)		15

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 1б. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	Зачетные единицы	Академические часы
Общая трудоемкость дисциплины	5	180
Аудиторные занятия (всего)		12
В том числе:		
Лекции		4
Практические занятия (ПЗ)		4
Лабораторные работы (ЛР)		4
Самостоятельная работа обучающихся (всего)		159+9 (экз.)
В том числе:		
Курсовая работа		30
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Другие виды самостоятельной работы: - подготовка к лабораторным работам		69
Другие виды самостоятельной работы: - подготовка к практическим работам		60
Текущий контроль успеваемости и промежуточная аттестация (зачет)		не предусмотрен
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		9 (экз.)
Практическая подготовка при реализации дисциплины (всего)		2

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	Основные угрозы информации	33	6	3	4	14+6(экз.)
2	Положения теории информационной безопасности информационных систем	61	8	3	8	24+18(экз.)
3	Методы обеспечения информационной безопасности	62	12	7	16	19+8(экз.)
4	Вопросы правового обеспечения защиты информации в информационных системах	24	4	2	2	12+4(экз.)
Всего на дисциплину		**180**	30	15	30	69+36 (экз.)

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	Основные угрозы информации	33	1	1	1,25	26,75+3(экз.)
2	Положения теории информационной безопасности информационных систем	61	1	1	1,25	55,75+2(экз.)
3	Методы обеспечения информационной безопасности	62	1	1	1,25	56,75+2(экз.)
4	Вопросы правового обеспечения	24	1	1	0,25	19,75+2(экз.)

	защиты информации в информационных системах					
Всего на дисциплину		**180**	4	4	4	159+9 (экз.)

5.2. Содержание дисциплины.

МОДУЛЬ 1 «Основные угрозы информации»:

Международные стандарты обмена информацией. Уязвимость информации. Понятие угрозы. Классификация угроз. Причины нарушения целостности информации. Физические угрозы безопасности информации. Аппаратные угрозы безопасности информации. Программные угрозы безопасности информации. Методы снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов. Методы несанкционированного доступа к электронной почте. Методы несанкционированного доступа к распределенным системам, построенным на основе архитектуры «клиент-сервер». Методы несанкционированного доступа к клиентскому программному обеспечению WWW. Особенности каналов утечки и несанкционированного доступа к информации в помещениях с информационными системами. Аппаратная реализация современных методов несанкционированного доступа к информации. Программная реализация несанкционированного доступа к информации на основе использования программных закладок. Использование компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации. Ботнеты. Darknet.

МОДУЛЬ 2 «Положения теории информационной безопасности информационных систем»:

Функции и задачи защиты информации. Основные положения теории информационной безопасности информационных систем. Понятие политики безопасности. Модели безопасности и их применение: модель Адепт-50; модель конечных автоматов; модель безопасности с полным перекрытием; модель Bell-LaPadula; модель Biba; модель Clark-Wilson; модель информационных потоков; модель невлияния; сетчатая модель; модель Brewer and Nesh; модель Graham-Denning; модель Harrison-Ruzzo-Ullman.

МОДУЛЬ 3 «Методы обеспечения информационной безопасности»:

Идентификация и аутентификация. Методы управления доступом к информации. Аудит, контроль целостности. Туннелирование. Криптографические методы защиты информации. Аппаратные и технические средства обеспечения безопасности информации. Программные средства обеспечения безопасности информации. Анализ мер обеспечения безопасности персонального компьютера. Анализ мер обеспечения безопасности файлового сервера. Анализ мер обеспечения безопасности сервера приложений. Методы и средства обеспечения безопасности в каналах информационно-вычислительных сетей и телекоммуникаций. Проектирование информационного обеспечения с учетом требований

информационной безопасности. Программные средства обеспечения безопасности информации. Организационное обеспечение информационной безопасности. Основные методы управления проектами защищенных информационных систем.

МОДУЛЬ 4 «Вопросы правового обеспечения защиты информации в информационных системах»:

Общая характеристика правового регулирования информации. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Основные законы и нормативные руководящие документы, касающиеся государственной тайны, информационной безопасности и защиты информации, нормативно-справочные документы. Лицензирование и сертификация как основа защиты информации

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 анализа угроз информации.	Программные средства анализа угроз безопасности информации объекта защиты	4
Модуль 2 **Цель:** формирование умений исследования моделей безопасности	Исследование моделей безопасности методами имитационного моделирования	8
Модуль 3 **Цель:** формирование умений проектирования и разработки защищенных информационных систем	Шифры на основе метода подстановок	6
	Шифры на основе метода гаммирования	4
	Стеганографические системы	4
	Обеспечение мер информационной безопасности в операционных системах и прикладных программах	2
Модуль 4 **Цель:** формирование умений выбора и обоснования проектных решений правового обеспечения	Разработка правового обеспечения защищенной информационной системы	2

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б. Лабораторные работы и их трудоемкость

Модули.	**Наименование**	**Трудоем**

Цели лабораторных занятий	лабораторных занятий	кость в часах
Модуль 1 **Цель:** формирование умений анализа угроз информации.	Программные средства анализа угроз безопасности информации объекта защиты	0,5
Модуль 2 **Цель:** формирование умений исследования моделей безопасности	Исследование моделей безопасности методами имитационного моделирования	0,25
Модуль 3 **Цель:** формирование умений проектирования и разработки защищенных информационных систем	Шифры на основе метода подстановок	0,5
	Шифры на основе метода гаммирования	0,5
	Стеганографические системы	0,5
	Обеспечение мер информационной безопасности в операционных системах и прикладных программах	0,5
Модуль 4 **Цель:** формирование умений выбора и обоснования проектных решений правового обеспечения	Разработка правового обеспечения защищенной информационной системы	0,25

5.4. Практические и (или) семинарские занятия.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4а. Тематика, форма практических занятий (ПЗ) и их трудоемкость

Модули. Цели практических занятий	Наименование практических занятий	Трудоем кость в часах
Модуль 1 **Цель:** Получение практических навыков анализа угроз информации.	Анализ угроз безопасности информации хранящейся в локальном компьютере	1
	Анализ угроз безопасности информации хранящейся в компьютере подключенном к локальной сети	2

Модуль 2 **Цель:** получение практических навыков построения моделей защиты информации	Построение модели Адепт-50 для локального компьютера	1
	Построение модели безопасности с полным перекрытием для компьютера подключенного к локальной сети	2
Модуль 3 **Цель:** освоение методов обеспечения информационной безопасности	Шифры на основе метода подстановок	2
	Шифрование с помощью датчика псевдослучайных чисел	1
	Изучение стандарта RSA	2
	Разработка комплекса мер по защите информации в офисе фирмы	2
Модуль 4 **Цель:** получение практических навыков работы с нормативно-правовой информацией	Анализ законодательства в сфере обеспечения информационной безопасности	2

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4б. Тематика, форма практических занятий (ПЗ) и их трудоемкость

Модули. **Цели практических занятий**	**Наименование практических занятий**	**Трудоемкость в часах**
Модуль 1 **Цель:** Получение практических навыков анализа угроз информации.	Анализ угроз безопасности информации хранящейся в локальном компьютере	0,5
	Анализ угроз безопасности информации хранящейся в компьютере подключенном к локальной сети	0,5
Модуль 2 **Цель:** получение практических навыков построения моделей защиты информации	Построение модели Адепт-50 для локального компьютера	0,5
	Построение модели безопасности с полным перекрытием для компьютера	0,5

	подключенного к локальной сети	
Модуль 3 **Цель:** освоение методов обеспечения информационной безопасности	Шифры на основе метода подстановок	0,25
	Шифрование с помощью датчика псевдослучайных чисел	0,5
	Изучение стандарта RSA	0,5
	Разработка комплекса мер по защите информации в офисе фирмы	0,5
Модуль 4 **Цель:** получение практических навыков работы с нормативно-правовой информацией	Анализ законодательства в сфере обеспечения информационной безопасности	0,25

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, экзамену в выполнении курсовой работы.

После вводных практических занятий, в которых обозначается содержание дисциплины, ее проблематика и практическая значимость, студентам выдается задание на курсовую работу.

Курсовая работа выполняется в соответствии с методическими указаниями по выполнению курсовой работы, разработанными на кафедре.

В рамках дисциплины выполняется 9 практических заданий, которые защищаются посредством устного опроса. Выполнение всех заданий обязательно.

В случае невыполнения практического задания по уважительной причине студент должен выполнить пропущенные практические занятия в часы, отведенные на консультирование с преподавателем.

В рамках дисциплины выполняется 7 лабораторных работ, 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, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-13960-0. - URL: https://urait.ru/bcode/496741 . - (ID=139087-0)
2. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А.В. Зенков. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-14590-8. - URL: https://urait.ru/bcode/497002 . - (ID=140920-0)
3. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие для учреждений ВПО : в составе учебно-методического комплекса / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 6-е изд. ; стер. - М. : Академия, 2012. - 331 с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Текст : непосредственный. - ISBN 978-5-7695-9222-5 : 366 р. 30 к. - (ID=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, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-12774-4. - URL: https://urait.ru/bcode/495922 . - (ID=135778-0)
2. Прохорова, О.В. Информационная безопасность и защита информации : учебник для вузов / О.В. Прохорова. - 3-е изд. - Санкт-Петербург [и др.] : Лань, 2021. - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-8114-7970-2. - URL: https://e.lanbook.com/book/169817 . - (ID=145977-0)
3. Внуков, А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. - 3-е изд. - Москва : Юрайт, 2023. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-534-07248-8. - URL: https://urait.ru/bcode/512268 . - (ID=135647-0)
4. 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. - ЦОР IPR SMART. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-238-02644-2. - URL: https://www.iprbookshop.ru/81535.html . - (ID=120865-0)
5. Фороузан, Б.А. Криптография и безопасность сетей : учебное пособие / Б.А. Фороузан; под редакцией А.Н. Берлина. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) : Ай Пи Ар Медиа, 2021. - ЦОР IPR SMART. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-4497-0946-2. - URL: https://www.iprbookshop.ru/102017.html . - (ID=146330-0)
6. Основы национальной безопасности : учебник по направл. подготовки 050100 «Педагогическое образование» (профиль «Безопасность жизнедеятельности», квалификация «бакалавр») / Л.А. Михайлов [и др.]; под ред. Л.А. Михайлова. - 2-е изд. ; испр. - М. : Академия, 2014. - 175 с. - (Высшее образование. Бакалавриат). - Текст : непосредственный. - ISBN 978-5-4468-0377-4 : 325 р. 60 к. - (ID=100981)
7. Бабаш, А.В. Информационная безопасность. Лабораторный практикум : учеб. пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - 2-е изд. ; стер. - Москва : КноРус, 2013. - 131 с. : ил. + 1 электрон. опт. диск (CD-ROM). - (Бакалавриат). - Текст : непосредственный. - ISBN 978-5-406-02760-8 : 270 р. - (ID=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. Оценочные средства промежуточной аттестации: экзамен дисциплины "Информационная безопасность и защита информации" направления подготовки 09.03.02 Информационные системы и технологии. Профиль: Информационные системы в административном управлении : в составе учебно-методического комплекса / Каф. Информационные системы ; разраб. И.В. Мартынов. - Тверь : ТвГТУ, 2017. - (УМК-В). - Сервер. - Текст : электронный. - (ID=129742-0)
3. Информационная безопасность : метод. указ. к выполнению курсового проекта для студентов второго курса направления "Прикл. информатика" / Тверской гос. техн. ун-т, Каф. ИС ; сост. В.В. Алексеев. - Тверь : ТвГТУ, 2015. - 16 с. - Текст : непосредственный. - 16 р. 60 к. - (ID=110069-95)
4. Информационная безопасность : метод. указ. к выполнению курсового проекта для студентов второго курса направления "Прикл. информатика" : в составе учебно-методического комплекса / Тверской гос. техн. ун-т, Каф. ИС ; сост. В.В. Алексеев. - Тверь : ТвГТУ, 2015. - (УМК-М). - Сервер. - Текст : электронный. - 0-00. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/109223 . - (ID=109223-1)
5. Учебно-методический комплекс дисциплины "Безопасность информационных технологий и систем". Направление подготовки 09.03.02 Информационные системы и технологии. Направленность (профиль): Разработка, внедрение и

сопровождение информационных систем : ФГОС 3++ / составитель И.В. Мартынов ; Кафедра "Информационные системы". - Тверь, 2022. - (УМК). - Текст : электронный. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/154224 . - (ID=154224-0)

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. Ресурсы:https://lib.tstu.tver.ru/header/obr-res
2. ЭКТвГТУ:https://elib.tstu.tver.ru/MegaPro/Web
3. ЭБС "Лань":https://e.lanbook.com/
4. ЭБС "Университетская библиотека онлайн":https://www.biblioclub.ru/
5. ЭБС «IPRBooks»:https://www.iprbookshop.ru/
6. Электронная образовательная платформа "Юрайт" (ЭБС «Юрайт»):https://urait.ru/
7. Научная электронная библиотека eLIBRARY:https://elibrary.ru/
8. Информационная система "ТЕХНОРМАТИВ". Конфигурация "МАКСИМУМ" : сетевая версия (годовое обновление): [нормативно-технические, нормативно-правовые и руководящие документы (ГОСТы, РД, СНиПы и др.]. Диск 1,2,3,4. - М. :Технорматив, 2014. - (Документация для профессионалов). - CD. - Текст : электронный. - 119600 р. – (105501-1)
9. База данных учебно-методических комплексов:https://lib.tstu.tver.ru/header/umk.html

УМК размещен: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/154224

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

1. Экзаменационный билет соответствует форме, утвержденной Положением о рабочих программах дисциплин, соответствующих федеральным государственным образовательным стандартам высшего образования с учетом профессиональных стандартов. Типовой образец экзаменационного билета приведен в Приложении. Обучающемуся даётся право выбора заданий из числа, содержащихся в билете, принимая во внимание оценку, на которую он претендует.

Число экзаменационных билетов – 17. Число вопросов (заданий) в экзаменационном билете – 3 (1 вопрос для категории «знать» и 2 вопроса для категории «уметь»).

Продолжительность экзамена – 60 минут.

2. Шкала оценивания промежуточной аттестации в форме экзамена – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

3. Критерии оценки за экзамен:

для категории «знать»:

выше базового – 2;

базовый – 1;

ниже базового – 0;

критерии оценки и ее значение для категории «уметь»:

отсутствие умения – 0 балл;

наличие умения – 2 балла.

«отлично» - при сумме баллов 5 или 6;

«хорошо» - при сумме баллов 4;

«удовлетворительно» - при сумме баллов 3;

«неудовлетворительно» - при сумме баллов 0, 1 или 2.

4. Вид экзамена – письменный экзамен, включающий решение задач с использованием ЭВМ.

5. База заданий, предъявляемая обучающимся на экзамене

1. Понятие угрозы. Классификация угроз безопасности
2. Международные стандарты обмена информацией. Понятие угрозы.
3. Особенности каналов утечки и несанкционированного доступа к информации в информационных системах. Аппаратная реализация современных методов несанкционированного доступа к информации.
4. Использование компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации.
5. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.
6. Методы и средства обеспечения безопасности в информационных системах.
7. Технические средства обеспечения безопасности ЭВМ.

8. Методы защиты информации от несанкционированного доступа в сетях ЭВМ.

9. Идентификация и аутентификация. Методы управления доступом к информации. Аудит, контроль целостности.

10. Криптографические методы защиты информации.

11. Аппаратные и технические средства обеспечения безопасности информации.

12. Программные средства обеспечения безопасности информации.

13. Проектирование информационного обеспечения с учетом требований информационной безопасности.

14. Программные средства обеспечения безопасности информации.

15. Организационное обеспечение информационной безопасности.

16. Общая характеристика правового регулирования информации. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

17. Основные законы и нормативные руководящие документы, касающиеся государственной тайны, информационной безопасности и защиты информации, нормативно-справочные документы.

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 на экзаменационные вопросы и решенных на компьютере задач задавать студенту в устной форме уточняющие вопросы в рамках содержания экзаменационного билета, выданного студенту.

Иные нормы, регламентирующие процедуру проведения экзамена, представлены в Положении о текущем контроле успеваемости и промежуточной аттестации студентов.

9.2. Оценочные средства для проведения промежуточной аттестации в форме зачета

Учебным планом зачет по дисциплине не предусмотрен.

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

1. Шкала оценивания курсовой работы (проекта) – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

2. Тема курсовой работы: «Разработка мер и средств по защите информации информации в ИС».

3. Критерии итоговой оценки за курсовую работу.

Таблица5. Оцениваемые показатели для проведения промежуточной аттестации в форме курсовой работы

№ раздела	Наименование раздела	Баллы по шкале уровня
	Термины и определения	Выше базового– 2

		Базовый – 1 Ниже базового – 0
	Введение	Выше базового– 2 Базовый – 1 Ниже базового – 0
1	Общая часть (обзор литературы по выбранной теме курсовой работы)	Выше базового–6 Базовый – 3 Ниже базового – 0
2	Специальная часть	Выше базового–10 Базовый – 6 Ниже базового – 0
	Заключение	Выше базового– 2 Базовый – 1 Ниже базового – 0
	Список использованных источников	Выше базового– 2 Базовый – 1 Ниже базового – 0

Критерии итоговой оценки за курсовую работу (проект):

«отлично» – при сумме баллов от 22 до 24;

«хорошо» – при сумме баллов от 17 до 20;

«удовлетворительно» – при сумме баллов от 12 до 16;

«неудовлетворительно» – при сумме баллов менее 11, а также при любой другой сумме, если по разделу «Специальная часть», работа имеет 0 баллов.

4. В процессе выполнения курсовой работы руководитель осуществляет систематическое консультирование.

5. Дополнительные процедурные сведения:

- студенты выбирают тему для курсовой работы самостоятельно из предложенного списка и согласовывают свой выбор с преподавателем в течение двух первых недель обучения;
- проверку и оценку работы осуществляет руководитель, который доводит до сведения обучающего достоинства и недостатки курсовой работы и ее оценку. Оценка проставляется в зачетную книжку обучающегося и ведомость для курсовой работы. Если обучающийся не согласен с оценкой руководителя, проводится защита работы перед комиссией, которую назначает заведующий кафедрой;
- защита курсовой работы проводится в течение двух последних недель семестра и выполняется в форме устной защиты в виде доклада и презентации на 5-7 минут с последующим ответом на поставленные вопросы, в ходе которых выясняется глубина знаний студента и самостоятельность выполнения работы;
- работа не подлежит обязательному внешнему рецензированию;
- курсовые работы хранятся на кафедре в течение трех лет.

10. Методические рекомендации по организации изучения дисциплины

Студенты перед началом изучения дисциплины ознакомлены с системами кредитных единиц и балльно-рейтинговой оценки.

Студенты, изучающие дисциплину, обеспечиваются электронными изданиями или доступом к ним, учебно-методическим комплексом по дисциплине, включая

методические указания к выполнению практических, лабораторных, курсовых работ, всех видов самостоятельной работы.

В учебный процесс рекомендуется внедрение субъект-субъектной педагогической технологии, при которой в расписании каждого преподавателя определяется время консультаций студентов по закрепленному за ним модулю дисциплины.

11. Внесение изменений и дополнений в рабочую программу дисциплины

Протоколами заседаний кафедры ежегодно обновляется содержание рабочих программ дисциплин, по утвержденной «Положением о рабочих программах дисциплин» форме.

Приложение

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Тверской государственный технический университет»

Направление подготовки бакалавров 09.03.02 Информационные системы и технологии.

Профиль подготовки – Разработка, внедрение и сопровождение информационных систем.

Кафедра Информационных систем.

Дисциплина «Безопасность информационных технологий и систем».

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №

1. Задание для проверки уровня «знать» – или 0, или 1, или 2 балла:
Основные виды вредоносных программ. Принцип их действия.

2. Задание для проверки уровня «уметь» – или 0, или 1 балл:
Охарактеризовать общие принципы построения политики безопасности учреждения.

3. Задача для проверки уровня «уметь» – или 0, или 2 балла:
Расширенный алгоритм Евклида для RSA.

Критерии итоговой оценки за экзамен:

«отлично» - при сумме баллов 5 или 6;
«хорошо» - при сумме баллов 4;
«удовлетворительно» - при сумме баллов 3;
«неудовлетворительно» - при сумме баллов 0, 1 или 2.

Составитель: доцент каф. ИС _____ И.В. Мартынов

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