

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)»
«Информационная безопасность»

Направление подготовки магистров 09.04.02 Информационные системы и технологии

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

Типы задач профессиональной деятельности: организационно-управленческий

Форма обучения – очная

Факультет информационных технологий
Кафедра «Информационные системы»

Тверь 2019

Рабочая программа дисциплины соответствует ОХОП подготовки магистров 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
«13» мая 2019 г., протокол № 5.

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 «Информационная безопасность» изучение теоретических и практических вопросов 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.

2. Место дисциплины в структуре ОП.

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)». Для изучения курса требуются знания дисциплин «Анализ и синтез информационных систем», «Компьютерные технологии», «Системная инженерия».

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-4. *Способен контролировать обеспечение качества, надежности и безопасности информационных систем.*

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИПК-4.2. Обеспечивает достаточный уровень безопасности информационных систем.

Показатели оценивания индикаторов достижения компетенций

Знать:

31. Способы анализа и выбора методов и средств обеспечения защищенности информации в информационных системах.

32. Методы обеспечения информационной безопасности;

33. Методы и средства безопасного хранения, переработки и трансляции информации.

Уметь:

У1. Проводить сравнительный анализ и выбор средств обеспечения защиты информации.

У2. Обосновывать организационно-технические мероприятия по защите информации в ИС.

Иметь опыт практической подготовки:

ПП1. Применения моделей безопасности информационных систем

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных, лабораторных и практических занятий; самостоятельная работа студента; 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	3	108
Аудиторные занятия (всего)		39
В том числе:		
Лекции		13
Практические занятия (ПЗ)		13
Лабораторные работы (ЛР)		13
Самостоятельная работа обучающихся (всего)		33+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		7
Другие виды самостоятельной работы: - подготовка к практическим работам		6
Текущий контроль успеваемости и промежуточная аттестация (зачет)		не предусмотрен
Текущий контроль успеваемости и промежуточная аттестация (экзамен)		36 (экз)
Практическая подготовка при реализации дисциплины (всего)		46
В том числе:		
Практические занятия (ПЗ)		13
Лабораторные работы (ЛР)		13
Курсовая работа		20
Курсовой проект		не предусмотрен

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	Особенности современных каналов утечки и несанкционированного доступа к	14	4	2	4	6+6(экз.)

	информации					
2	Положения теории информационной безопасности	84	7	9	9	21+24(экз.)
3	Вопросы правового обеспечения защиты информации	10	2	2	-	6+6(экз.)
Всего на дисциплину		108	13	13	13	33+36 (экз.)

5.2. Содержание дисциплины.

МОДУЛЬ 1 «Особенности современных каналов утечки и несанкционированного доступа к информации»:

Международные стандарты обмена информацией. Понятие угрозы. Классификация угроз безопасности.

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 информационных системах. 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.

МОДУЛЬ 2 «Положения теории информационной безопасности»:

Понятия информационной безопасности и защиты информации.

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.

Методы и средства обеспечения безопасности в информационных системах.

Технические средства обеспечения безопасности ЭВМ. Анализ мер обеспечения безопасности персонального компьютера.

Методы защиты информации от несанкционированного доступа в сетях ЭВМ.

МОДУЛЬ 3 «Вопросы правового обеспечения защиты информации»:

Понятие национальной безопасности. 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.

5.3. Лабораторные работы

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а. Лабораторные работы и их трудоемкость

Порядковый номер модуля. Цели лабораторных работ	Наименование лабораторных работ	Трудоемкость в часах
Модуль 1 Цель: изучение методов анализа защищенности информации.	Количественная оценка стойкости парольной защиты	4
Модуль 2 Цель: изучение методов защиты информации	Элементы криптографии	5
	Алгоритмы работы с большими числами	4

5.4. Практические и (или) семинарские занятия.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

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

Порядковый номер модуля. Цели практических работ	Примерная тематика занятий и форма их проведения	Трудоемкость в часах
Модуль 1 Цель: изучение методов анализа угроз информации.	Анализ угроз безопасности информации объекта защиты	2
Модуль 2 Цель: изучение основных моделей защиты информации	Построение модели безопасности с полным перекрытием для объекта требующего защиты	5
	Анализ криптографического алгоритма RSA	4
Модуль 3 Цель: получение практических навыков работы с нормативно-правовой информацией	Анализ законодательства в сфере защиты информации	2

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 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 4 практических задания, 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 3 лабораторные 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, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - 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. - 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. - ISBN 978-5-534-12774-4. - URL: <https://urait.ru/bcode/495922>. - (ID=135778-0)
2. Внуков, А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. - 3-е изд. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - ISBN 978-5-534-07248-8. - URL: <https://urait.ru/bcode/490277>. - (ID=135647-0)
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. - ЦОР IPR SMART. - Текст : электронный. - ISBN 978-5-238-02644-2. - URL: <http://www.iprbookshop.ru/81535.html>. - (ID=120865-0)
4. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/157578> . - (ID=146329-0)
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. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102017.html>. - (ID=146330-0)
6. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - ISBN 978-5-9916-9043-0. - URL: <https://urait.ru/bcode/491249> . - (ID=145962-0)
7. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72444.html>. - (ID=146331-0)
8. 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=100981-2)

9. 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 p. - (ID=96781-8)

7.3. Методические материалы

1. Конспект лекций по дисциплине "Защита информации в информационных системах". Направление подготовки 09.04.02 Информационные системы и технологии. Профиль: Информационные системы в административном управлении : в составе учебно-методического комплекса / Каф. Информационные системы ; разработ. В.В. Алексеев. - Тверь : ТвГТУ, 2017. - (УМК-Л). - Сервер. - Текст : электронный. - (ID=129668-0)
2. 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 p. 60 к. - (ID=110069-95)
3. 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: <http://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/109223>. - (ID=109223-1)
4. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие / А.В. Моргунов; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2019. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-7782-3918-0. - URL: <https://e.lanbook.com/book/152227>. - (ID=145943-0)
5. Учебно-методический комплекс дисциплины "Информационная безопасность" направления подготовки 09.04.02 Информационные системы и технологии. Направленность (профиль)– Разработка, внедрение и сопровождение информационных систем / Каф. Информационные системы ; сост. В.В. Алексеев. - 2022. - (УМК). - Текст : электронный. - 0-00. - URL: <https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro129740>. - (ID=129740-1)

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 Community.

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. ЭК ТвГТУ: <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/129740>

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 обязательно).

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

10. 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.

Таблица 5. 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

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

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

Направление подготовки магистров 09.04.02 Информационные системы и
технологии

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

Кафедра «Информационные системы»

Дисциплина «Информационная безопасность»

Семестр 3

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Вопрос для проверки уровня «ЗНАТЬ» – 0 или 1 или 2 балла:

Понятие угрозы. Классификация угроз безопасности.

2. Задание для проверки уровня «УМЕТЬ» по разделу «Вопросы правового обеспечения защиты информации в базах и хранилищах данных» - 0 или 1 или 2 балла:

Провести правовой анализ ситуации: сотрудник установил на своем рабочем компьютере не лицензионную копию программного обеспечения.

3. Задание для проверки уровня «УМЕТЬ» – 0 или 1 или 2 балла:

Построить линейный конгруэнтный датчик. Проанализировать криптостойкость полученной гаммы шифра.

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

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