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

Направление подготовки магистров 09.04.03 Прикладная информатика
Направленность (профиль)– Прикладная информатика в радиолокационных и управляющих системах
Типы задач профессиональной деятельности: научно-исследовательский

Форма обучения – очная

Факультет информационных технологий
Кафедра Радиотехнические информационные системы

Тверь 20____

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
«____» _____ 20___г., протокол № ___.

Заведующий кафедрой РИС: д.т.н., профессор _____ С.Ф. Боев

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

Начальник отдела
комплектования
зональной научной библиотеки О.Ф. Жмыхова

Начальник управления
информационных ресурсов
и технологий

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 элективной части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)». Для изучения курса требуются знания дисциплин «Математическое моделирование», «Компьютерные технологии», «Методология и технология проектирования информационных систем».

Приобретенные знания в рамках данной дисциплины необходимы в дальнейшем при написании магистерской диссертации.

3. Планируемые результаты обучения по дисциплине.

3.1. Планируемые результаты обучения по дисциплине.

Компетенция, закрепленная за дисциплиной в ОХОП:

ПК-2Способен выполнять моделирование объектов и процессов с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ.

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИПК-2.1. Применяет физические, математические модели и методы моделирования сигналов, процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем.

Показатели оценивания индикаторов достижения компетенций

Знать:

З1. Способы анализа и выбора методов и средств обеспечения защищенности информации в процессе применения физических, математических моделей и методы моделирования сигналов, процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем.

З2. Методы обеспечения информационной безопасности;

Уметь:

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

У2. Обосновывать мероприятия по защите информации в процессе применения физических, математических моделей и методы моделирования сигналов, процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем.

Иметь опыт практической подготовки:

ПП1. Применения моделей безопасности информационных систем

3.2. Технологии, обеспечивающие формирование компетенций

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

4. Трудоемкость дисциплины и виды учебной работы.

Таблица 1. 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		10
Практические занятия (ПЗ)		20
Лабораторные работы (ЛР)		не предусмотрены
Самостоятельная работа обучающихся (всего)		42
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Другие виды самостоятельной работы: - подготовка к практическим работам		22
Текущий контроль успеваемости и промежуточная аттестация (зачет)		20
Практическая подготовка при реализации дисциплины (всего)		20
Практические занятия (ПЗ)		20
Лабораторные работы (ЛР)		не предусмотрены
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен

5. Структура и содержание дисциплины.

5.1. Структура дисциплины

Таблица 2. 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 информации	18	4	4	-	10
2	Положения теории информационной безопасности	42	4	14	-	24
3	Вопросы правового обеспечения защиты информации	12	2	2	-	8
Всего на дисциплину		**72**	10	20	-	42

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.

Особенности каналов утечки и несанкционированного доступа к информации впроцессе применения физических, математических моделей и методы моделирования сигналов, процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем. 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 впроцессе применения физических, математических моделей и методы моделирования сигналов, процессов и явлений, лежащих в основе принципов действия радиотехнических устройств и систем.

Технические средства обеспечения информационной безопасности. Анализ мер обеспечения информационной безопасности.

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

Учебным планом лабораторные работы не предусмотрены

5.4. Практические занятия.

Таблица 4. 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	4
	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, поискулитературы, 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 занятиям, к текущему контролю успеваемости, зачету.

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.

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 [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)
4. Мельников, Д.А. Информационная безопасность открытых систем : учебник для вузов по направлению "Прикладная информатика" / Д.А. Мельников. - 2-е изд. ; стер. - Москва : Флинта, 2014. - ЭБС Университетская библиотека онлайн. - Текст : электронный. - Дата обращения: 07.07.2022. - Режим доступа: по подписке. - ISBN 978-5-9765-1613-7. - URL: https://biblioclub.ru/index.php?page=book_view_red&book_id=363419. - (ID=113594-0)

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. 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)
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. - 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)
4. 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)
5. 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)
6. Нестеров, С.А.Основы информационной безопасности : учебное пособие / С.А. Нестеров. - 5-е изд. ; стер. - Санкт-Петербург [и др.] : Лань, 2022. - (Учебники для вузов. Специальная литература). - ЭБС Лань. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 25.08.2022. - ISBN 978-5-8114-4067-2. - URL: https://e.lanbook.com/book/206279. - (ID=113816-0)
7. 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)
8. 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. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ISBN 978-5-7782-3918-0. - URL: https://e.lanbook.com/book/152227 . - (ID=145943-0)

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 ; разраб. В.В. Алексеев. - Тверь : ТвГТУ, 2017. - (УМК-Л). - Сервер. - Текст : электронный. - (ID=129668-0)

2. Информационная безопасность : методические указания к выполнению курсовой работы для студентов третьего курса направления «Прикладная информатика» / Тверской государственный технический университет, Кафедра Информационные системы ; составители: В.В. Алексеев, Д.В. Мартынов. - Тверь : ТвГТУ, 2022. - 16 с. - Сервер. - Текст : электронный. - 0-00. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/146511 . - (ID=146511-1)
3. 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)
4. 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)
5. 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)
6. Информационная безопасность : метод. указ. к выполнению курс. проекта для студентов 3 курса спец. "Прикл. информатика (в экономике)" и "Информ. системы и технологии" / сост. В.В. Алексеев ; Тверской гос. техн. ун-т, Каф. ИС. - Тверь : ТвГТУ, 2005. - 16 с. - Сервер. - Текст : электронный. - [б. ц.]. - (ID=58741-1)
7. Информационная безопасность : метод. указ. к выполнению курс. проекта для студентов 3 курса спец. "Прикл. информатика (в экономике)" и "Информ. системы и технологии" / сост. В.В. Алексеев ; Тверской гос. техн. ун-т, Каф. ИС. - Тверь : ТвГТУ, 2005. - 16 с. - Библиогр. : с. 14 - 15. - Текст : непосредственный. - 7 р. 30 к. - (ID=57119-94)
8. Учебно-методический комплекс дисциплины "Информационная безопасность". Направление подготовки 09.04.03 Прикладная информатика. Направленность (профиль): Прикладная информатика в радиолокационных и управляющих системах : ФГОС 3++ / Кафедра "Радиотехнические информационные системы" ; сост. В.В. Алексеев. - 2022. - (УМК). - Текст : электронный. - URL: https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/152726. - (ID=152726-0)

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.

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/152726

8. Материально-техническое обеспечение дисциплины

Кафедра 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 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 информационной безопасности.

7. Технические средства обеспеченияинформационной безопасности.

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 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 не предусмотрены.

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

Содержание рабочих программ дисциплин ежегодно обновляется протоколами заседаний кафедры по утвержденной «Положением о структуре, содержании и оформлении рабочих программ дисциплин по образовательным программам, соответствующим ФГОС ВО с учетом профессиональных стандартов» форме.

Приложение

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

Направление подготовки магистров 09.04.03 Прикладная информатика

Направленность (профиль) – Прикладная информатика в радиолокационных и управляющих системах

Кафедра «Радиотехнические информационные системы»

Дисциплина «Информационная безопасность»

ЗАДАНИЕ ДЛЯ ДОПОЛНИТЕЛЬНОГО ИТОГОВОГО КОНТРОЛЬНОГО ИСПЫТАНИЯ №_1__

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

Понятие угрозы. Классификация угроз безопасности.

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

Методы и средства обеспечения безопасности в радиотехнических системах и комплексах.

1. Задание для проверки уровня «УМЕТЬ» – 0 или 1 балл:

Построить линейный конгруэнтный датчик. Проанализировать криптостойкость полученной гаммы шифра.

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 РИС: д.т.н., профессор _____ С.Ф. Боев