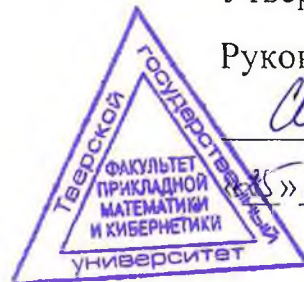


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 30.09.2023 14:35:30
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

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

Утверждаю:

Руководитель ООП



С.М. Дудаков С.М. Дудаков

«30» августа 2021 г.

Рабочая программа дисциплины (с аннотацией)

Основы информационной безопасности

Направление подготовки

09.03.03 – «Прикладная информатика»

Направленность (профиль)

«Прикладная информатика в мехатронике»

Для студентов 4 курса

очная форма

Составитель: к.ф.-м.н. Кудряшов М.Ю.

Тверь, 2021

I. Аннотация

1. Цель и задачи дисциплины

Цель освоения дисциплины:

— сформировать системное представление об информационной безопасности.

Задачами освоения дисциплины являются:

— усвоение системы знаний о базовых основах информационной безопасности;

— формирование умений реализовывать прикладные знания в области информационной безопасности в профессиональной деятельности;

— совершенствование методических навыков использования средств информационной безопасности в профессиональной деятельности.

2. Место дисциплины в структуре ООП

Данная дисциплина относится к разделу «Информатика и информационно-коммуникационные технологии» обязательной части Блока 1.

Для успешного освоения дисциплины «Основы информационной безопасности» от обучающегося требуются знания и навыки, полученные в результате изучения курсов по алгебре, математическому анализу, дискретной математике, языкам программирования. Данная дисциплина необходима для изучения дисциплины «Проектирование, разработка и эксплуатация информационных систем».

3. Объем дисциплины: 3 зачетных единиц, 108 академических часов, в том числе:

контактная аудиторная работа: практические занятия 30 часов, в т.ч. практическая подготовка 0 часов, лабораторные работы 30 часов, в т.ч. практическая подготовка 0 часов;

контактная внеаудиторная работа: контроль самостоятельной работы _____, в том числе курсовая работа _____;

самостоятельная работа: 48 часов, в том числе контроль 0 часов.

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

| Планируемые результаты освоения образовательной программы (формируемые компетенции) | Планируемые результаты обучения по дисциплине |
|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и | ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> | <p>культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p> |
| <p>ОПК-6 Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования</p> | <p>ОПК-6.1 Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования</p> <p>ОПК-6.2 Применяет методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий</p> <p>ОПК-6.3 Владеет навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий</p> |

5. Форма промежуточной аттестации и семестр прохождения - зачет, 8 семестр.

6. Язык преподавания русский.

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

| Учебная программа – наименование разделов и тем | Всего (час.) | Контактная работа (час.) | | | | | Самостоятельная работа, в том числе Контроль (час.) |
|----------------------------------------------------|-----------------|--------------------------|-----------------------------------|----------------------------------------------------|-----------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------|
| | | Лекции | | Практические занятия/ Лабораторные работы | | Контроль самостоятельной работы (в том числе курсовая работа) | |
| | | всего | В т.ч. практическая подготовка | всего | В т.ч. практическая подготовка | | |
| Основные положения | 8 | 0 | 0 | 2/2 | 0 | 0 | 4 |
| Формальные модели шифров | 8 | 0 | 0 | 2/2 | 0 | 0 | 4 |
| Оценка стойкости блочных шифров | 8 | 0 | 0 | 2/2 | 0 | 0 | 4 |
| Шифр Rijndael (AES) | 8 | 0 | 0 | 2/2 | 2/2 | 0 | 4 |
| Распределение симметричных ключей | 12 | 0 | 0 | 4/4 | 2/2 | 0 | 4 |
| Криптографические хеш- функции | 12 | 0 | 0 | 4/4 | 4/4 | 0 | 4 |
| Схемы открытого шифрования и их стойкость | 8 | 0 | 0 | 2/2 | 0 | 0 | 4 |
| Двухключевые криптосистемы | 12 | 0 | 0 | 4/4 | 2/2 | 0 | 4 |
| Схемы цифровой подписи и их стойкость | 16 | 0 | | 4/4 | 2/2 | 0 | 8 |
| Безопасность сети | 16 | 0 | 0 | 4/4 | 2/2 | 0 | 8 |
| ИТОГО | 108 | 0 | 0 | 30/30 | 14/14 | 0 | 48 |

III. Образовательные технологии

| Учебная программа – наименование разделов и тем (в строгом соответствии с разделом II РПД) | Вид занятия | Образовательные технологии |
|--------------------------------------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------|
| Основные положения | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Формальные модели шифров | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Оценка стойкости блочных шифров | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Шифр Rijndael (AES) | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Распределение симметричных ключей | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Криптографические хеш-функции | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Схемы открытого шифрования и их стойкость | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Двухключевые криптосистемы | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
| Схемы цифровой подписи и их стойкость | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |

| | | |
|-------------------|-------------------------------------------|-----------------------------------------------------------|
| Безопасность сети | Практические занятия, лабораторные работы | 1. Изложение теоретического материала 2. Решение задач |
|-------------------|-------------------------------------------|-----------------------------------------------------------|

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Для проведения текущей и промежуточной аттестации:

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

ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Написание рефератов по проблемам обеспечения информационной безопасности современных информационных систем

Критерии оценивания:

Оригинальность текста составляет свыше 75% - 3 балла

Оригинальность текста составляет 50-74 % - 2 балла

Оригинальность текста составляет 25-49 % - 1 балл

Оригинальность текста составляет менее 25% - 0 баллов

привлечены ли наиболее известные работы по теме исследования (в т.ч. публикации последних лет) – 2 балла

реферат опирается на учебную литературу и/ или устаревшие издания – 1 балл

Отражение в плане ключевых аспектов темы – 2 балла;

Фрагментарное отражение ключевых аспектов темы – 1 балл;

Полное соответствие содержания теме и плану реферата – 2 балла;

Частичное соответствие содержания теме и плану реферата – 1 балла;

сопоставление различных точек зрения по одному вопросу (проблеме) – 1 балла;

Все представленные выводы обоснованы – 2 балла;

Аргументирована часть выводов – 1 балл.

верно оформлены ссылки на используемую литературу – 1 балл

соблюдены правила орфографической, пунктуационной, стилистической культуры – 1 балл;

соблюдены требования к объёму реферата – 1 балл.

ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Написание рефератов по методам обеспечения информационной безопасности от несанкционированного доступа

Критерии оценивания:

Оригинальность текста составляет свыше 75% - 3 балла

Оригинальность текста составляет 50-74 % - 2 балла

Оригинальность текста составляет 25-49 % - 1 балл

Оригинальность текста составляет менее 25% - 0 баллов

привлечены ли наиболее известные работы по теме исследования (в т.ч. публикации последних лет) – 2 балла

реферат опирается на учебную литературу и/ или устаревшие издания – 1 балл

Отражение в плане ключевых аспектов темы – 2 балла;

Фрагментарное отражение ключевых аспектов темы – 1 балл;

Полное соответствие содержания теме и плану реферата – 2 балла;

Частичное соответствие содержания теме и плану реферата – 1 балла;

сопоставление различных точек зрения по одному вопросу (проблеме) – 1 балла;

Все представленные выводы обоснованы – 2 балла;

Аргументирована часть выводов – 1 балл.

верно оформлены ссылки на используемую литературу – 1 балл

соблюдены правила орфографической, пунктуационной, стилистической культуры – 1 балл;

соблюдены требования к объёму реферата – 1 балл.

ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Решение задач по математическим основам обеспечения информационной безопасности от несанкционированного доступа

Имеется полное верное доказательство, включающее правильный ответ – 3 балла

Дано верное решение, но получен неправильный ответ из-за арифметической ошибки – 2 балла

Имеется верное решение части задачи из-за логической ошибки – 1 балл

Решение не дано – 0 баллов

ОПК-6 Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования

ОПК-6.1 Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования

Решение задач по математическим основам обеспечения целостности информации

Критерии оценивания:

Дан правильный развернутый ответ – 2 балла;

Ответ содержит неточности – 1 балл.

Решение не дано – 0 баллов

ОПК-6.2 Применяет методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий

Решение задач по математическим основам криптографических методов защиты информации Решение задач на представления чисел в различных системах счисления и кодировках

Критерии оценивания:

Дан правильный развернутый ответ – 2 балла;

Ответ содержит неточности – 1 балл.

Решение не дано – 0 баллов

ОПК-6.3 Владеет навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий

Решение задач по методам и средствам обеспечения информационной безопасности компьютерных систем Критерии оценивания:

Дан правильный развернутый ответ – 2 балла;

Ответ содержит неточности – 1 балл.

Решение не дано – 0 баллов

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857.html>

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>

3. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие/ Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011.— 260 с.— Режим доступа: <http://www.iprbookshop.ru/26486.html>

4. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: <http://www.iprbookshop.ru/13936.html>

б) Дополнительная литература

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: <http://www.iprbookshop.ru/10677.html>

2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183.html>

2) Программное обеспечение

а)

Список ПО в 4б

Перечень программного обеспечения (со свободными лицензиями): Adobe Acrobat Reader DC, Anaconda3 2019.07 (Python 3.7.3 64-bit), Apache Tomcat 8.0.27, Cadence SPB/OrCAD 16.6, GlassFish Server Open Source Edition 4.1.1, Google Chrome, IntelliJ IDEA, IIS 10.0 Express, Java SE Development Kit 8 Update 191 (64-bit), JetBrains PyCharm Community Edition 2019.2.1, Kaspersky Endpoint Security для Windows, Lazarus 2.0.12, MiKTeX, NetBeans IDE 8.2, Notepad++ (64-bit x64), ONLYOFFICE Desktop Editors 7.1 (x64), Origin 8.1 Sr2, Python 3.10.7, R for Windows 3.6.1, RStudio Desktop, Visual Studio Community 2022, VLC media player, WinDjView 2.1, Unreal Commander v3.57x64

Список ПО в 249

Перечень программного обеспечения (со свободными лицензиями): Adobe Acrobat Reader DC, Google Chrome, Kaspersky Endpoint Security для Windows,

ONLYOFFICE Desktop Editors 7.1 (x64), Python 3.10.7, R for Windows 3.6.1, RStudio Desktop, Visual Studio Community 2022, VLC media player, Unreal Commander v3.57x64

б) Свободно распространяемое программное обеспечение

3) Современные профессиональные базы данных и информационные справочные системы

ЭБС «**ZNANIUM.COM**» www.znanium.com;

ЭБС «**Университетская библиотека онлайн**» <https://biblioclub.ru/>;

ЭБС «**Лань**» <http://e.lanbook.com>.

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

Интернет-университет <http://www.intuit.ru>

VI. Методические материалы для обучающихся по освоению дисциплины

Важной составляющей данного раздела РПД являются требования к рейтинг-контролю с указанием баллов, распределенных между модулями и видами работы обучающихся.

Максимальная сумма баллов по учебной дисциплине, заканчивающейся зачетом, по итогам семестра составляет 100 баллов (50 баллов - 1-й модуль и 50 баллов - 2-й модуль).

Студенту, набравшему 40 баллов и выше по итогам работы в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший до 39 баллов включительно, сдает зачет.

Распределение баллов по модулям устанавливается преподавателем и может корректироваться.

Пример заданий для промежуточной аттестации:

Планы и методические указания

Задания:

1. Криптоанализ криптограмм методом частотного анализа
2. Криптоанализ криптограмм методом вероятных слов
3. Криптоанализ аддитивных шифров
4. Стеганография и стеганографический анализ изображений

6. Линейный криптоанализ блочных алгоритмов шифрования
7. Дифференциальный криптоанализ блочных алгоритмов шифрования

Вопросы к зачету:

- Правовые аспекты обеспечения информационной безопасности.
- Средства обеспечения информационной безопасности.
- Основные организационные мероприятия в сфере обеспечения информационной безопасности.
- Технические средства обеспечения информационной безопасности.
- Методы и средства защиты от несанкционированного доступа.
- Криптографические методы защиты информации.
- Защита информации в компьютерных сетях.
- Вирусы и обеспечение безопасности от вирусных атак.
- Основные методы криптографического анализа.
- Компьютерная стеганография в контексте обеспечения защиты информации.
- Основные методы стеганографического анализа.

VII. Материально-техническое обеспечение

Для аудиторной работы

| | |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Учебная аудитория № 310 (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)</p> | <p>Набор учебной мебели, экран проектор.</p> |
| <p>Учебная аудитория № 304 (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)</p> | <p>Набор учебной мебели, экран, комплект аудиотехники (радиосистема, стационарный микрофон с настольным держателем, усилитель, микшер, акустическая система), проектор, ноутбук.</p> |

Для самостоятельной работы.

| | |
|-------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| <p>Помещение для самостоятельной работы обучающихся: Компьютерный класс факультета ПМиК № 249</p> | <p>Набор учебной мебели, компьютер, проектор.</p> |
|-------------------------------------------------------------------------------------------------------|---------------------------------------------------|

170002, Тверская обл., г.Тверь,
Садовый переулок, д.35

VIII. Сведения об обновлении рабочей программы дисциплины

| № п.п. | Обновленный раздел рабочей программы дисциплины | Описание внесенных изменений | Дата и протокол заседания кафедры, утвердившего изменения |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| 1. | 3. Объем дисциплины | Выделение часов на практическую подготовку | От 29.10.2020 года, протокол № 3 ученого совета факультета |
| 2. | II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий | Выделение часов на практическую подготовку | От 29.10.2020 года, протокол № 3 ученого совета факультета |
| 3. | 3. Объем дисциплины. II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий | Изменения в учебные планы и обновление рабочих программ практик, рабочих программ дисциплин в части включения часов практической подготовки. | Решение научно-методического совета (протокол №1 от 09.09.2020 г.). |
| 4. | 4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы | Изменения в учебные планы и в рабочие программы дисциплин, формирующих новые/измененные компетенции в соответствии с приказом Минобрнауки России | Решение научно-методического совета (протокол №6 от 02.06.2021 г.) |

| | | | |
|---|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------|
| | | от 26.11.2020 г. №1456. | |
| 5 | V. Учебно-методическое и информационное обеспечение, необходимое для проведения практики 2) Программное обеспечение | Внесены изменения программное обеспечение | в От 29.09.2022 года, протокол № 2 ученого совета факультета |
| 6 | VII. Материально-техническое обеспечение | Внесены изменения материально-техническое обеспечение аудиторий | в От 29.09.2022 года, протокол № 2 ученого совета факультета |