

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 09.10.2023 16:00:58
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

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

Утверждаю:
Руководитель ООП
С.М. Дудаков
2021 г.



Рабочая программа дисциплины (с аннотацией)

Основы информационной безопасности

Направление подготовки

09.03.03 Прикладная информатика

Направленность (профиль)

Прикладная информатика в экономике

Для студентов 3 курса

Форма обучения очная

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: лекции 20 часов, в т.ч. практическая подготовка -, лабораторные работы 20 часов, в т.ч. практическая подготовка -;

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

самостоятельная работа: 68 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 библиографической культуры с	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

<p>применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p>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		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	2	0	2	0	0	4
Формальные модели шифров	8	2	0	2	0	0	4
Оценка стойкости блочных шифров	8	2	0	2	0	0	4
Шифр Rijndael (AES)	8	2	0	2	0	0	8
Распределение симметричных ключей	12	2	0	2	0	0	8
Криптографические хеш- функции	12	2	0	2	0	0	8
Схемы открытого шифрования и их стойкость	8	2	0	2	0	0	8
Двухключевые криптосистемы	12	2	0	2	0	0	8
Схемы цифровой подписи и их стойкость	16	2		2	0	0	8
Безопасность сети	16	2	0	2	0	0	8
ИТОГО	108	20	0	20	0	0	68

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

Компьютерный класс факультета прикладной математики и кибернетики № 249 (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
FidesysBundle 1.4.43 x64	Акт приема передачи по договору №02/12-13 от 16.12.2013
Google Chrome	бесплатно
JetBrains PyCharm Community Edition 4.5.3	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011

MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012
MiKTeX 2.9	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
OpenOffice	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»
Python 3.4.3	бесплатно
Python 3.5.1 (Anaconda3 2.5.0 64 bit)	бесплатно
R for Windows 3.3.2	бесплатно
STATGRAPHICS Centurion XVI.И	Акт приема-передачи № Tr024185 от 08.07.2010
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

Компьютерный класс факультета прикладной математики и кибернетики № 46 (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	
Adobe Acrobat Reader DC - Russian	бесплатно
Apache Tomcat 8.0.27	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
GlassFish Server Open Source Edition 4.1.1	бесплатно
Google Chrome	бесплатно
Java SE Development Kit 8 Update 45 (64-bit)	бесплатно
JetBrains PyCharm Community Edition 4.5.3	бесплатно
JetBrains PyCharm Edu 3.0	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
NetBeans IDE 8.0.2	бесплатно
NetBeans IDE 8.2	бесплатно
Notepad++	бесплатно

Oracle VM VirtualBox 5.0.2	бесплатно
Origin 8.1 Sr2	договор №13918/М41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»
Python 3.1 pygame-1.9.1	бесплатно
Python 3.4 numpy-1.9.2	бесплатно
Python 3.4.3	бесплатно
Python 3.5.1 (Anaconda3 2.5.0 64-bit)	бесплатно
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
R Studio	бесплатно
Anaconda3 2019.07 (Python 3.7.3 64-bit)	бесплатно

б) Свободно распространяемое программное обеспечение

Компьютерная лаборатория факультета ПМиК № 201а (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Перечень программного обеспечения (со свободными лицензиями): Linux Kubuntu, KDE, TeXLive, TeXStudio, LibreOffice, GIMP, Gwenview, ImageMagick, Okular, Skanlite, Google Chrome, KDE Connect, Konversation, KRDC, KTorrent, Thunderbird, Elisa, VLC media player, PulseAudio, KAppTemplate, KDevelop, pgAdmin4, PostgreSQL, Qt, QtCreator, R, RStudio, Visual Studio Code, Perl, Python, Ruby, clang, clang++, gcc, g++, nasm, flex, bison, Maxima, Octave, Dolphin, HTop, Konsole, KSystemLog, Xterm, Ark, Kate, KCalc, Krusader, Spectacle, Vim
--	---

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 экзаменом, по итогам семестра составляет 60 баллов (30 баллов - 1-й модуль и 30 баллов - 2-й модуль).

Обучающемуся, набравшему 40–54 балла, при подведении итогов семестра (на последнем занятии по дисциплине) в рейтинговой ведомости учета успеваемости и зачетной книжке может быть выставлена оценка «удовлетворительно».

Обучающемуся, набравшему 55–57 баллов, при подведении итогов семестра (на последнем занятии по дисциплине) в графе рейтинговой ведомости учета успеваемости «Премияльные баллы» может быть добавлено 15 баллов и выставлена экзаменационная оценка «хорошо».

Обучающемуся, набравшему 58–60 баллов, при подведении итогов семестра (на последнем занятии по дисциплине) в графе рейтинговой ведомости учета успеваемости «Премияльные баллы» может быть добавлено 27 баллов и выставлена экзаменационная оценка «отлично». В каких-либо иных случаях добавление премиальных баллов не допускается.

Обучающийся, набравший до 39 баллов включительно, сдает экзамен.

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

Компьютерная лаборатория факультета ПМиК № 201а (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Набор учебной мебели, доска маркерная, компьютер, сервер (системный блок), концентратор сетевой.
--	--

Для самостоятельной работы

Помещение для самостоятельной работы обучающихся: Компьютерный класс факультета ПМиК № 4б (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Компьютер, экран, проектор, кондиционер.
Компьютерный класс №2 факультета ПМиК № 249 (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Набор учебной мебели, компьютер, проектор.

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	Выделение часов на практическую подготовку	От 29.10.2020 года, протокол № 3

	темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий		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 от 26.11.2020 г. №1456.	Решение научно-методического совета (протокол №6 от 02.06.2021 г.)
5	I. Аннотация. IV. Оценочные материалы для проведения текущей и промежуточной аттестации	Изменения в учебные планы и в рабочие программы дисциплин, формирующих новые/ измененные компетенции в соответствии с приказом Минобрнауки России от 26.11.2020 г. № 1456	Протокол № 7 заседания ученого совета от 30.12.2021 года
6	V. Учебно-методическое и информационное обеспечение, необходимое для проведения практики	Внесены изменения в программное обеспечение	От 29.09.2022 года, протокол № 2 ученого совета факультета

	2) Программное обеспечение		
7	VII. Материально-техническое обеспечение	Внесены изменения в материально-техническое обеспечение аудиторий	От 29.09.2022 года, протокол № 2 ученого совета факультета
	VII. Материально-техническое обеспечение	Внесены изменения в материально-техническое обеспечение аудиторий	От 22.08.2023 г., протокол № 1 заседания ученого совета факультета