

Аннотация дисциплины

Б1.В.04 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки бакалавров

01.03.02 «Прикладная математика и информатика»

Курс 4 Семестр 7 Трудоемкость 3 з.е.

1.1 Цель дисциплины: развитие логического мышления, овладение основными методами обеспечения информационной безопасности, в том числе криптографических, умение самостоятельно расширять знания в области обеспечения информационной безопасности.

1.2 Задачи дисциплины

- изучение основных понятий и методов решения типовых задач информационной безопасности;
- овладение практическими навыками в реализации информационной безопасности.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к части, формируемой участниками образовательных отношений (Б1.В) учебного плана.

Для изучения данной учебной дисциплины (модуля) студент должен владеть обязательным минимумом содержания математической части ООП для данного направления:

знать/понимать

- основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, принципы алгоритмизации и программирования;

уметь

- применять математические методы для решения практических задач;
- составлять алгоритмы и компьютерные программы;

владеть

- методами решения алгебраических уравнений, аналитической геометрии, теории вероятностей;
- инструментальными средствами программирования.

Вышеуказанные знания, умения и навыки формируются предшествующими дисциплинами:

- Алгебра и аналитическая геометрия.
- Математический анализ.
- Основы программирования.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

- Новые информационные технологии в экономике.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
Знать ИУК-3.1 (Зн.1) Проблемы подбора эффективной команды ИУК-3.3 (Зн.3) Основы стратегического управления человеческими ресурсами,	Уметь ИУК-3.13 (06.001 D/03.06 У.3) Осуществлять осуществлять социальное взаимодействие, коммуникации с заинтересованными сторонами Владеть

Код и наименование индикатора*	Результаты обучения по дисциплине
нормативные правовые акты, касающиеся организации и осуществления профессиональной деятельности ИУК-3.4 (Зн.4) Модели организационного поведения, факторы формирования организационных отношений ИУК-3.5 (Зн.5) Стратегии и принципы командной работы, основные характеристики организационного климата и взаимодействия людей в организации	ИУК-3.15 (В.1) Организацией и управлением командным взаимодействием в решении поставленных целей ИУК-3.18 (В.4) Составлением деловых писем с целью организации и сопровождения командной работы
ПК-4 Способен активно участвовать в разработке системного и прикладного программного обеспечения	
Знать ИПК-4.1 (06.001 D/03.06 Зн.1) Принципы построения архитектуры системного и прикладного программного обеспечения и виды архитектуры системного и прикладного программного обеспечения ИПК-4.5 (06.015 В/16.5 Зн.3) Архитектура, устройство и функционирование вычислительных систем используемых в разработке системного и прикладного программного обеспечения ИПК-4.7 (06.016 А/06.6 Зн.1) Возможности ИС, предметная область системное и прикладное программное обеспечение ИПК-4.8 (06.016 А/30.6 Зн.1) Управление рисками проекта при разработке системного и прикладного программного обеспечения ИПК-4.9 (06.016 А/30.6 Зн.2) Возможности ИС, методы разработки прикладного программного обеспечения	Уметь ИПК-4.10 (06.001 D/03.06 У.1) Использовать существующие типовые решения и шаблоны проектирования системного и прикладного программного обеспечения ИПК-4.12 (06.016 А/30.6 У.2) Планировать работы в проектах разработки системного и прикладного программного обеспечения Владеть ИПК-4.17 (06.016 А/30.6 Тд.1) Качественный анализ рисков при разработке системного и прикладного программного обеспечения
ПК-8 Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции	
Знать ИПК-8.2 (06.016 А/30.6 Зн.1) Управление рисками проекта, способы планирования необходимых ресурсов и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции ИПК-8.3 (40.001 А/02.5 Зн.3) Методы, этапы и средства планирования и организации исследований и разработок ИПК-8.4 (06.015 В/16.5 У.1) Устанавливать программное обеспечение	Уметь ИПК-8.5 (06.016 А/06.6 У.1) Разрабатывать документы, составлять соответствующие технические описания и инструкции ИПК-8.6 (06.016 А/30.6 У.2) Планировать работы в проектах, необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий ИПК-8.7 (40.001 А/02.5 У.2) Оформлять результаты научно-исследовательских и опытно-конструкторских работ, составлять соответствующие технические описания и инструкции Владеть ИПК-8.9 (06.016 А/06.6 Тд.1) Подготовка договоров в проектах в соответствии с типовой формой, составление соответствующих технических описаний и инструкций ИПК-8.12 (40.001 А/02.5 Др.2 Тд.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, планирование необходимых ресурсов и этапов выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Содержание и структура дисциплины

№ раз-дела	Наименование разделов, тем	Количество часов				
		Все го	Аудиторная работа			Внеауди-торная ра-бота
			Л	ПЗ	ЛР	
1.	Введение в основы информационной безопасности	6	2	-	2	2
	<i>1. Исторический обзор применения средств сокрытия информации. История криптографии.</i>	6	2	-	2	2
2.	Основные классы шифров и их свойства	16	6	-	6	4
	<i>1. Шифры перестановки.</i>	6	2	-	2	2
	<i>2. Блочные шифры замены</i>	10	4	-	4	2
3.	Надёжность шифров	12	4	-	4	4
	<i>Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Практически стойкие шифры.</i>	12	4	-	4	4
4.	Методы синтеза и анализа симметричных шифр-систем	20	8	-	8	4
	<i>1. Управление открытыми ключами.</i>	10	4	-	4	2
	<i>2 Методы анализа криптографических алгоритмов.</i>	10	4	-	4	2
5.	Методы синтеза и анализа асимметричных крип-тосистем	20	8	-	8	4
	<i>1 Системы шифрования с открытым ключом.</i>	10	4	-	4	2
	<i>2 Алгоритмы идентификации на основе асим-метричных криптосистем.</i>	10	4	-	4	2
6.	Хеш-функции и их криптографические приложе-ния	14	6	-	6	2
	<i>Хеш-функции и аутентификация сообщений. Об-щие сведения о хеш-функциях.</i>	14	6	-	6	2
	ИТОГО по разделам дисциплины:	88	34	0	34	20
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	15,8				
	Общая трудоемкость по дисциплине	108				

Сокращения: Л – лекции, ПЗ – практические занятия, ЛР – лабораторные работы, СРС – самостоятельная работа студентов.

Курсовые проекты или работы: не предусмотрены

Интерактивные образовательные технологии, используемые в аудиторных заня-тиях: Лекционные материалы реализуются с помощью электронных презентаций. При ре-ализации учебной работы по дисциплине «Основы информационной безопасности» ис-пользуются следующие образовательные технологии: интерактивная подача материала с мультимедийной системой; разбор конкретных исследовательских задач.

Вид аттестации: зачет.

Основная литература

1. Фомичев, В. М. Криптография — наука о тайнописи: учебное пособие / В. М. Фомичев. - Москва: Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст: электронный. - Режим доступа: <https://znanium.com/read?id=389799>
2. Бабаш, А. В. Криптографические методы защиты информации. Т.1: Уч.-метод. пос./Бабаш А. В., 2-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст: электронный. - Режим доступа: <https://znanium.com/read?id=334834>

Дополнительная литература

3. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. С.О. Крамарова. — Москва: РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1716-6>. - ISBN 978-5-369-01716-6. — Текст: электронный. - Режим доступа: <https://znanium.com/read?id=416723>

Периодические издания:

1. Базы данных компании «Ист Вью» <http://dlib.eastview.com>
2. Электронная библиотека GREBENNIKON.RU <https://grebennikon.ru/>

Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» <https://urait.ru/>
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» <http://www.biblioclub.ru/>
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

Профессиональные базы данных

1. Scopus <http://www.scopus.com/>
2. ScienceDirect <https://www.sciencedirect.com/>
3. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
4. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
5. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
6. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
7. Президентская библиотека им. Б.Н. Ельцина <https://www.prlib.ru/>
8. База данных CSD Кембриджского центра кристаллографических данных (CCDC) <https://www.ccdc.cam.ac.uk/structures/>
9. Springer Journals: <https://link.springer.com/>
10. Springer Journals Archive: <https://link.springer.com/>
11. Nature Journals: <https://www.nature.com/>
12. Springer Nature **Protocols and Methods:** <https://experiments.springernature.com/sources/springer-protocols>
13. Springer Materials: <http://materials.springer.com/>
14. Nano Database: <https://nano.nature.com/>
15. Springer eBooks (i.e. 2020 eBook collections): <https://link.springer.com/>
16. "Лекториум ТВ" <http://www.lektorium.tv/>
17. Университетская информационная система РОССИЯ <http://uisrussia.msu.ru>

Информационные справочные системы

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа

1. КиберЛенинка <http://cyberleninka.ru/>;
2. Американская патентная база данных <http://www.uspto.gov/patft/>
3. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
4. Федеральный портал "Российское образование" <http://www.edu.ru/>;
5. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru/>;
6. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/> .
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" <https://pushkininstitute.ru/>;
8. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
9. Служба тематических толковых словарей <http://www.glossary.ru/>;
10. Словари и энциклопедии <http://dic.academic.ru/>;
11. Образовательный портал "Учеба" <http://www.ucheba.com/>;
12. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--plai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ

1. Электронный каталог Научной библиотеки КубГУ <http://megapro.kubsu.ru/MegaPro/Web>
2. Электронная библиотека трудов ученых КубГУ <http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6>
3. Среда модульного динамического обучения <http://moodle.kubsu.ru>
4. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://infoneeds.kubsu.ru/>
5. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
6. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
7. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" <http://icdau.kubsu.ru/>

Автор: доцент кафедры прикладной математики, к.т.н., Савин В.Н.