

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.16 Основы информационной безопасности»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.04 Программная инженерия
(код и наименование направления подготовки)

Разработка программно-информационных систем
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Заочная

Год набора 2021

Рабочая программа дисциплины «Б1.Д.Б.16 Основы информационной безопасности» рассмотрена и утверждена на заседании кафедры

Кафедра программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры

протокол № 9 от "11" 05 2021 г.

Заведующий кафедрой

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

наименование кафедры

подпись

Н.А. Соловьев

расшифровка подписи

Исполнители:

доцент

должность

подпись

Н.А. Тишина

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

09.03.04 Программная инженерия

код наименование

личная подпись

Н.А. Соловьев

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

личная подпись

Н.Н. Бигалиева

расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

И.В. Крючкова

расшифровка подписи

№ регистрации _____

© Тишина Н.А., 2021

© ОГУ, 2021

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

обучение студентов фундаментальным понятиям, основным определениям и методам обеспечения информационной безопасности организаций в условиях широкого применения современных информационных технологий.

Задачи:

- формирование знаний об исходных положениях теории информационной безопасности; об угрозах информационной безопасности, о законодательстве и стандартах в области информационной безопасности и о вредоносном программном обеспечении
- формирование умений анализировать угрозы информационной безопасности, использовать нормативные правовые документы по информационной безопасности, использовать средства обнаружения вредоносного программного обеспечения
- привитие навыков применения теоретических знаний для решения практических задач в области обеспечения информационной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Отсутствуют*

Постреквизиты дисциплины: *Б1.Д.В.15 Защита компьютерных систем*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
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-В-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 ОПК-3-В-2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: принципы, терминологию, составляющие, требования (критерии) информационной безопасности; нормативно-правовые основы информационной безопасности; вредоносное программное обеспечение Уметь: решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	2 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	8,25	8,25
Лекции (Л)	4	4
Практические занятия (ПЗ)	4	4
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: <i>- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;</i> <i>- подготовка к практическим занятиям;</i> <i>- подготовка к рубежному контролю</i>	135,75	135,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

Разделы дисциплины, изучаемые в 2 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в теорию информационной безопасности	52	1	3		48
2	Нормативно-правовые основы информационной безопасности	49	2	1		46
3	Вредоносное программное обеспечение	43	1			42
	Итого:	144	4	4		136
	Всего:	144	4	4		136

4.2 Содержание разделов дисциплины

1 Введение в теорию информационной безопасности

Задачи и принципы информационной безопасности; базовые понятия; составляющие информационной и компьютерной безопасности; информационная война; угрозы, риски, уязвимость; контроль доступа

2 Нормативно-правовые основы информационной безопасности

Стандарты, группы стандартов, обзор международных и Российских стандартов; ТЗИ в Российской Федерации.

Ответственность за нарушение информационной безопасности; компьютерное пиратство; обзор российского законодательства в области информационной безопасности.

3 Вредоносное программное обеспечение

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1.	1	Анализ проблем безопасности программно-информационных систем	1
2.	1	Стойкость парольной защиты	1
3.	1	Программная реализация и исследование простых криптографических алгоритмов	1
4.	2	Анализ зарубежных и Российских стандартов информационной безопасности	1
		Итого:	4

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Тишина, Н. А. Защита информационных процессов в компьютерных системах [Электронный ресурс]: учебное пособие для обучающихся по образовательным программам высшего образования по направлениям подготовки 09.03.01 Информатика и вычислительная техника и 09.03.04 Программная инженерия / Н. А. Тишина; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2019. - 179 с. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/94201_20190515.pdf

2 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: <https://znanium.com/catalog/product/402686>

5.2 Дополнительная литература

3 Мельников, В. П. Защита информации [Текст] : учебник для подготовки бакалавров по направлению 230100 "Информатика и вычислительная техника" / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; под ред. В. П. Мельникова. - Москва : Академия, 2014. - 297 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 291-293. - ISBN 978-5-4468-0332-3. (10)

4 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. (12)

5 Семененко, В. А. Программно-аппаратная защита информации: учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.(15)

5.3 Периодические издания

Вестник компьютерных и информационных технологий : журнал. - М. : Агентство "Роспечать", 2018-2020.

Информационно-измерительные и управляющие системы : журнал. - М. : Агентство "Роспечать", 2018-2020.

Информационные технологии : журнал. - М. : Агентство "Роспечать", 2018-2020.

1. Программные продукты и системы : журнал. - М. : Агентство "Роспечать", 2018-2020.

5.4 Интернет-ресурсы

- ФСТЭК России. Федеральная служба по техническому и экспортному контролю <http://fstec.ru/>

Информация об уязвимостях <http://www.iso27000.ru/katalog-ssylok/informaciya-ob-uyazvimostyah>

- Информационный портал по ИТ безопасности <http://www.securitylab.ru/>

- Информационный сайт: Безопасник <http://bezopasnik.org/article>

- Виртуальные учебные курсы и сайты дистанционного образования:

• Интернет университет информационных технологий:
https://www.intuit.ru/studies/courses?service=0&option_id=9&service_path=1

- Энциклопедии и справочные сайты:

• Свободная энциклопедия https://ru.wikipedia.org/wiki/Информационная_безопасность
<https://www.lektorium.tv/course/22929> - «Лекториум», Курс лекций: Сложность вычислений и основы криптографии

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

- Банк данных угроз безопасности информации ФСТЭК РОССИИ <https://bdu.fstec.ru/threat>

- База данных угроз безопасности информации [Common Vulnerabilities and Exposures \(CVE\)](http://cve.mitre.org/data/downloads/index.html)
<http://cve.mitre.org/data/downloads/index.html>

- ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2016]. – Режим доступа в сети ОГУ для установки системы: [\\fileserver1\GarantClient\garant.exe](http://fileserver1\GarantClient\garant.exe)

- КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2016]. – Режим доступа к системе в сети ОГУ для установки системы: [\\fileserver1\CONSULT\cons.exe](http://fileserver1\CONSULT\cons.exe)

- Операционная система Microsoft Windows

- OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

- Средства для разработки и проектирования: Microsoft Visual Studio.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный компьютерной техникой, удовлетворяющей требованиям к конфигурации аппаратного обеспечения используемых программ.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой, подключенной к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ОГУ.