

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.30 Информационная безопасность и защита информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.02 Фундаментальная информатика и информационные технологии
(код и наименование направления подготовки)

Разработка и администрирование информационных систем
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2024

Рабочая программа дисциплины «Б1.Д.Б.30 Информационная безопасность и защита информации» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
исполняемое кафедрой

протокол № 8 от "25" мая 2024г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем

наименование кафедры  подпись И.В. Влацкая расшифровка подписи

Исполнители:

Доцент  подпись Ю.Д. Фот расшифровка подписи

должность должность расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки
02.03.02 Фундаментальная информатика и информационные технологии

КБЭ - наименование  личная подпись А.Е. Шухман расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

 личная подпись Н.Н. Бигалиева расшифровка подписи

Уполномоченный по качеству института

 личная подпись И.В. Крючкова расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: ознакомление студентов с содержательной стороной проблемы информационной безопасности, изучение возможных путей обеспечения информационной безопасности применительно к информационным системам.

Задачи:

- **иметь представление** об основных возможностях систем информационной безопасности; методах описания систем информационной безопасности; принципах проектирования систем информационной безопасности; о возможности использования систем информационной безопасности.

- **должен знать** содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей; принципы обеспечения информационной безопасности в свете положений Доктрины информационной безопасности Российской Федерации, основные нормативные и руководящие документы в этой области; принципы системного анализа и классификации угроз информационной безопасности; существующие средства и методы обеспечения информационной безопасности; основные понятия проектирования систем информационной безопасности; принципы и методологию проектирования и использования систем информационной безопасности при решении различных прикладных задач; содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; правила лицензирования и сертификации в области защиты информации; виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

- **уметь** применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий, применить знания методологии при проектировании систем информационной безопасности.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.1 Философия, Б1.Д.Б.12 Физика*

Постреквизиты дисциплины: *Б1.Д.Б.27 Компьютерное моделирование*

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-5 Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	ОПК-5-В-3 Обеспечивает информационную безопасность информационных систем	Знать: задачи и методы исследования и обеспечения качества и надежности программных компонентов информационных систем и баз данных; основные положения законодательства РФ в области защиты информации, нормативно-правовую базу, отечественные и зарубежные

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		<p>стандарты в области информационной безопасности;</p> <p>положения стандартов Единой системы конструкторской документации, Единой системы программной документации, основные отечественные и зарубежные стандарты в области информационной безопасности, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и информационных систем.</p> <p>Уметь: реализовывать процессы жизненного цикла информационных систем с учетом основных требований информационной безопасности; применять нормативную базу и стандарты в области обеспечения информационной безопасности информационных систем;</p> <p>Владеть: навыками оценки и анализа функционирования средств и информационных систем и баз данных с учетом основных требований информационной безопасности; навыками работы с нормативными правовыми актами и стандартами.</p>

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	108	108
Контактная работа:	34,25	34,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - <i>написание реферата (Р);</i> - <i>самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);</i> - <i>изучение разделов курса «Информационная безопасность и защита информации» в системе электронного обучения;</i> - <i>изучение разделов массового открытого онлайн-курса «Информационная безопасность»;</i> - <i>подготовка к практическим занятиям;</i> - <i>подготовка к рубежному контролю.</i>	73,75	73,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. Государственная система правового обеспечения защиты информации в Российской Федерации	15	4	2		9
2	Режим защиты государственной тайны	9	2	2		5
3	Режим защиты конфиденциальной информации.	46	8	8		20
4	Информационная безопасность объектов критической информационной инфраструктуры.	24	2	2		20
5	Проектирование систем защиты информационных систем и баз данных	14	2	2		20
	Итого:	108	18	16		74
	Всего:	108	18	16		74

4.2 Содержание разделов дисциплины

№1 Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. Государственная система правового обеспечения защиты информации в Российской Федерации

Понятие, структура информационного правоотношения. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Проблемы информационной безопасности.

Общая характеристика информационно-правовых норм. Органы законодательства, регламентирующие деятельность по информационной безопасности. Понятие и виды защищаемой информации по российскому законодательству. Информация как объект гражданских прав.

№2 Режим защиты государственной тайны

Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

№3 Режим защиты конфиденциальной информации

Регуляторы в области защиты ПДн. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Ответственность за нарушение обработки ПДн. Ответственность за нарушение режима защиты персональных данных.

Коммерческая тайна. Сущность, задачи и особенности защиты коммерческой тайны. Меры по обеспечению защиты коммерческой тайны. Работа с информацией, составляющей коммерческую тайну. Коммерческая тайна в трудовых отношениях. Классификация мер защиты коммерческой тайны. Ответственность за нарушение коммерческой тайны.

Понятие интеллектуальной собственности. Объекты интеллектуальной собственности. Субъекты права на объекты интеллектуальной собственности. Права на объекты интеллектуальной собственности (интеллектуальные права). Области интеллектуальной собственности. Защита интеллектуальной собственности. Ответственность за правонарушения в области защиты интеллектуальной собственности.

Служебная тайна. Профессиональная тайна. Тайна следствия и судопроизводства. Отличие служебной тайны от профессиональной. Требования к защите служебной и профессиональной тайны. Ответственность за нарушение режима защиты служебной тайны. Ответственность за нарушение режима защиты профессиональной тайны.

№4 Информационная безопасность объектов критической информационной инфраструктуры

Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Правовые основы обеспечения безопасности КИИ Российской Федерации. Объекты и субъекты КИИ. Категорирование объектов критической информационной инфраструктуры. Оформление и передача в ФСТЭК России результатов категорирования. Обеспечение безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Контроль за обеспечением безопасности значимого объекта КИИ. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

№5 Проектирование систем защиты информационных систем и баз данных

Концептуальные основы для проектирования системы обеспечения безопасности информации. Программное, информационное и технологическое и организационное обеспечение системы защиты. Технологический процесс функционирования системы защиты информации от несанкционированного доступа, как комплекса программно-технических средств и организационных (процедурных) решений.

4.3 Практические занятия (семинары)

№ ЛР	№ раздела	Тема	Кол-во часов
1	1	Понятия и виды защищаемой информации	2
2	2	Режим защиты государственной тайны. Ответственность за нарушение режима защиты государственной тайны.	2
3	3	Нормативно-правовая база в области защиты ПДн. Проектирование системы защиты ИСПДн в соответствии с требованиями нормативно-методической базы. Ответственность за нарушение режима защиты персональных данных.	2
4	3	Меры по обеспечению защиты коммерческой тайны. Ответственность за нарушение коммерческой тайны.	2
5	3	Защита интеллектуальной собственности. Ответственность за правонарушения в области защиты интеллектуальной собственности.	2
6	3	Требования к защите служебной и профессиональной тайны. Ответственность за нарушение области защиты служебной и профессиональной тайн.	2
7	4	Обследование критической информационной инфраструктуры в соответствии с ФЗ №187. Категорирование объектов критической информационной инфраструктуры	2
8	5	Программное, информационное и технологическое и	2

№ ЛР	№ раздела	Тема	Кол-во часов
		организационное обеспечение системы защиты.	
		Итого:	16

5.1 Основная литература

1. Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/159977> (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей.

2. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/254168> (дата обращения: 09.03.2024). — Режим доступа: для авториз. пользователей.

3. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова.- 6-е изд., стер. - Москва : Академия, 2012. - 332 с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5.

5.2 Дополнительная литература

1. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/216425> (дата обращения: 09.03.2024). — Режим доступа: для авториз. пользователей.

2. Каширская, Е. Н. Защита информации в информационно - управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167621> (дата обращения: 09.03.2024). — Режим доступа: для авториз. пользователей.

3. Киренберг, Информационная безопасность современных операционных систем : учебное пособие / Киренберг, Г. А. . — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/295736> (дата обращения: 09.03.2024). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

1. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР
2. Защита информации. Инсайд : журнал. - Москва : ИД "Афина"

5.4 Интернет-ресурсы

1. <http://www.fsb.ru> – сайт ФСБ РФ
2. <http://www.fstec.ru> – сервер ФСТЭК РФ
3. <http://www.gov.ru> – сервер органов государственной власти РФ
4. <http://www.minsvyaz.ru> – сайт министерства информационных технологий и связи РФ
5. <http://www.scrf.gov.ru> – сайт Совета Безопасности РФ
6. www.consultant.ru – Консультант плюс
7. <https://gost.ru> – Росстандарт
8. <http://docs.cntd.ru> – Электронный фонд правовой и нормативно-технической документации
9. <http://www.securrity.ru> – Сайт Информационная безопасность
10. <https://www.securitylab.ru> – Информационный портал по информационной безопасности
11. <https://securelist.ru/> - Сетевая штаб-квартира экспертов «Лаборатории Касперского»
12. <https://openedu.ru/course/hse/DATPRO/> - «Открытое образование». Курсы, MOOK: Защита информации.

13. <https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii> - «Coursera». Курсы, МО-ОК: Методы и средства защиты информации

14. <https://openedu.ru/course/ITMOUniversity/INFSEC/> - «Открытое образование». Курсы, МО-ОК: «Информационная безопасность»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

а) программно- аппаратное обеспечение:

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021

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

б) базы данных, информационно-справочные и поисковые системы:

– Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ <\\fileserv1\!CONSULT\cons.exe>

– Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа <\\fileserv1\GarantClient\garant.exe>. В локальной сети ОГУ.

– Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : <http://pravo.fso.gov.ru/ips/>, в локальной сети ОГУ.

– Открытые поисковые системы.

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, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

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

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.