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.24 Организационное и правовое обеспечение информационной безопасности»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2022

Рабочая программа дисциплины «*Б1.Д.Б.24 Организационное и правовое обеспечение информационной безопасности*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "14" марта 2022 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнитель:
Доцент *должность* *подпись* Ю.Д. Фот *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
подпись Н.Н. Бигалиева *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись И.В. Крючкова *расшифровка подписи*

№ регистрации 140741

© Фот Ю.Д., 2022
© ОГУ, 2022

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: совершенствование знаний, умений и навыков обучающихся, а также получение ими дополнительных знаний, умений и навыков по вопросам организационного и правового обеспечения информационной безопасности.

Задачи:

1) теоретический компонент:

– знать основы организационной и правовой защиты информации, ее современные проблемы и терминологию;

– изучить руководящие документы по обеспечению режима секретности и конфиденциальности на объекте;

– получить базовые представления о типовой структуре службы безопасности, ее основные задачи и функции должностных лиц;

– знать основные документы, регламентирующую организационную безопасность на объекте;

2) познавательный компонент:

– оценивать состояние организационной защиты информации на объекте;

– определять рациональные меры по обеспечению организационной и правовой защиты на объекте;

– организовать работу персонала с конфиденциальной информацией.

3) практический компонент:

– иметь навыки выявления угроз информационной безопасности объекта;

– обеспечения режима секретности и конфиденциальности на объекте.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика, Б1.Д.Б.22 Основы информационной безопасности, Б1.Д.Б.39 Право*

Постреквизиты дисциплины: *Б1.Д.Б.36 Стандарты информационной безопасности, Б1.Д.В.6 Обеспечение безопасности объектов критической информационной инфраструктуры, Б2.П.В.П.2 Преддипломная практика*

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 применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5-В-1 Знает источники и классификацию угроз информационной безопасности ОПК-5-В-2 Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в	**Знать:** нормативно-методическую базу в области национальной безопасности РФ; структуру государственной системы защиты информации; информационное

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	России ОПК-5-В-3 Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации ОПК-5-В-4 Знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-5-В-5 Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-5-В-6 Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	законодательство, юридические механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну и конфиденциальную информацию. **Уметь:** осуществлять анализ безопасности компьютерных систем на соответствие отечественным и зарубежным нормативно-правовым документам в области компьютерной безопасности; проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем на основе нормативно-правовой базы регуляторов; **Владеть:** правовыми нормами реализации профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	ОПК-6-В-1 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной Информации, по аттестации объектов информатизации и сертификации средств защиты информации ОПК-6-В-2 Знает систему организационных мер, направленных на защиту информации ограниченного доступа ОПК-6-В-3 Знает нормативные, руководящие и методические документы	**Знать:** основы экономических знаний при расчете ущерба информационной безопасности компьютерным системам на основе нормативно-правовой базы, определять рациональные меры по обеспечению организационной и правовой защиты; организационные, технические и

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
экспортному контролю	уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа ОПК-6-В-6 Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-6-В-7 Умеет определить политику контроля доступа работников к информации ограниченного доступа ОПК-6-В-8 Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации ОПК-6-В-9 Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	программно-аппаратные методы защиты информации; **Уметь:** разрабатывать формализованные модели, методы и алгоритмы решения типовых задач безопасности компьютерных систем в соответствии с отечественными и зарубежными стандартами; оценивать риски информационной безопасности; **Владеть:** знаниями по документальному обеспечению деятельности оператора; навыками анализа и разработки моделей безопасности компьютерных систем.

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:	**53,25**	**53,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	34	34
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;*	**54,75**	**54,75**

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
- подготовка к рубежному контролю.		
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ 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	10	2	2		6
2	Государственная система правового обеспечения защиты информации в Российской Федерации	12	2	4		6
3	Режим защиты государственной тайны	10	2	2		6
4	Защита персональных данных	14	2	6		6
5	Режим защиты государственных информационных систем	12	2	4		6
6	Защита интеллектуальной собственности	12	2	4		6
7	Аттестация объектов информатизации по требованиям безопасности информации.	12	2	4		6
8	Лицензирование и система сертификации средств защиты информации	12	2	4		6
9	Ответственность за правонарушения в области информационной безопасности	14	2	4		8
	Итого:	108	18	34		56
	Всего:	108	18	34		56

4.2 Содержание разделов дисциплины

№1 Роль и место информационной безопасности в системе национальной безопасности Российской Федерации

Понятие, структура информационного правоотношения. Стратегия национальной безопасности Российской Федерации. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Стратегии развития информационного общества в Российской Федерации.

№2 Государственная система правового обеспечения защиты информации в Российской Федерации

Общая характеристика информационно-правовых норм. Органы законодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской. Федерации. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Понятие и виды защищаемой информации по российскому законодательству. Информация как объект гражданских прав.

№3 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.

№4 Защита персональных данных

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. Частная 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.

№5 Режим защиты государственных информационных систем

Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации.

№6 Защита интеллектуальной собственности

Интеллектуальная собственность и история ее правовой охраны в России. Правовое регулирование авторских прав и прав, смежных с авторскими. Патентное право. Международные соглашения в области охраны интеллектуальной собственности. Право на использование объектов интеллектуальной собственности, составляющих единую технологию. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (Роспатент): правовая основа деятельности, структура, функции. Права на программы для ЭВМ и базы данных. Понятие и правовой режим программ для ЭВМ и баз данных. Субъекты прав на программы для ЭВМ и базы данных. Содержание прав на программы для ЭВМ и базы данных. Исключительное право на программу для ЭВМ или базу данных, созданную по договору заказа либо при выполнении работ по договору подрядного типа

№7 Аттестация объектов информатизации по требованиям безопасности информации.

Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная). Участники аттестации и их полномочия (компетенции). Задачи, функции права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

№8 Лицензирование и система сертификации средств защиты информации

Организационно-правовые основы лицензирования деятельности по защите информации. Лицензирование деятельности технической и криптографической защите информации. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки;

информации, технических средств контроля защищенности информации, программных, аппаратных; средств защиты информации, программных средств контроля защищенности информации. Особенности сертификации средств защиты информации от утечки по техническим каналам. Особенности сертификации средств защиты информации от НСД.

№9 Ответственность за правонарушения в области информационной безопасности

Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области конфиденциальной информации.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации	2
2	2	Органы законодательства, регламентирующие деятельность по информационной безопасности	2
2	3	Виды информации ограниченного доступа	2
3	4	Режим защиты государственной тайны	2
4	5	Особенности обработки персональных данных. Нормативно-правовая база в области защиты ПДн.	2
4	6	Построение частной модели угроз безопасности ИСПДн	2
4	7	Проектирование системы защиты ИСПДн в соответствии с требованиями нормативно-методической базы	2
5	8	Нормативно-правовая база в области защиты государственных информационных систем	2
5	9	Проектирование системы защиты государственных информационных систем	2
6	10	Законодательство об охране интеллектуальной собственности	2
6	11	Права на программы для ЭВМ и базы данных.	2
7	12	Аттестация объектов информатизации по требованиям безопасности информации	2
7	13	Порядок аттестации объектов информатизации (автоматизированных систем) на соответствие требованиям безопасности	2
8	14	Организационно-правовые основы лицензирования деятельности по защите информации.	2
8	15	Особенности сертификации средств защиты информации	2
9	16,17	Ответственность за правонарушения в области информационной безопасности	4
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Организационно-правовое обеспечение информационной безопасности: учебное пособие. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. / Под ред. А.А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.

5.2 Дополнительная литература

1. Правовое обеспечение информационной безопасности [Текст] : учеб. пособие для вузов / под ред. С. Я. Казанцева.- 2-е изд., испр. и доп. - М. : Академия, 2007. - 240 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 234. - ISBN 978-5-7695-3635-9.
2. Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182279 (дата обращения: 28.03.2022). — Режим доступа: для авториз. пользователей.
3. Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности : методические указания / А. В. Крыжановский. — Самара : ПГУТИ, 2018. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182281 (дата обращения: 28.03.2022). — Режим доступа: для авториз. пользователей.
4. Мальцев, В. А. Правовое обеспечение информационной безопасности в российской федерации : учебно-методическое пособие / В. А. Мальцев. — Воронеж : ВГУ, 2017. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154824 (дата обращения: 28.03.2022). — Режим доступа: для авториз. пользователей.

5.3 Периодические издания

Журналы:
- «Информационная безопасность»;
- «Вестник информационной безопасности»;
- «Проблемы информационной безопасности. Компьютерные системы».

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://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle
13. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК: Защита информации.
14. https://ru.coursera.org/learn/metody-i-sredstva-zashity-informacii - «Coursera». Курсы, МООК: Методы и средства защиты информации
15. https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti - «Coursera». Курсы, МООК: Менеджмент информационной безопасности
16. https://www.intuit.ru/studies/courses/3648/890/info – «Интуит. Национальный открытый университет» Курсы, МООК: Аттестация объектов информатизации по требованиям безопасности информации.
17. https://www.intuit.ru/studies/courses/3601/843/info - «Интуит. Национальный открытый университет» Курсы, МООК: Информационное право: Информация.
18. https://openedu.ru/course/ITMOUniversity/INTPRO/- «Открытое образование» Курсы, МООК: Правовые основы защиты интеллектуальной собственности.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

а) программно- аппаратное обеспечение:

1. Операционная система Microsoft Windows

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 \\fileserver1\!CONSULT\cons.exe

– Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа \\fileserver1\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.

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.

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.