Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ОД.8 Информационная безопасность и защита информации»

Уровень высшего образования

БАКАЛАВРИАТ

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

Общий профиль
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 4 от "29" 11 2016 г.

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

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

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.02 Фундаментальная информатика и информационные технологии
код наименование *личная подпись* А.Е.Шухман *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись Н.Н. Грицай *расшифровка подписи*

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

№ регистрации 48103

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: ознакомление студентов с содержательной стороной проблемы информационной безопасности, как основной составляющей национальной 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 обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.19 Введение в информатику, Б.1.Б.20 Основы программирования, Б.1.Б.22 Архитектура вычислительных систем, Б.1.Б.24 Компьютерные сети, Б.1.В.ОД.6 Операционные системы*

Постреквизиты дисциплины: *Б.1.В.ДВ.3.1 Методы защиты информации, Б.2.В.П.2 Практика по получению профессиональных умений и опыта профессиональной деятельности*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: основы информационной безопасности и защиты информации **Уметь:** применять стандарты информационной безопасности при применении информационных технологий **Владеть:** нормативно-правовой базой и стандартами информационной безопасности	ОПК-1 способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
	с фундаментальной информатикой и информационными технологиями
Знать: основы информационной безопасности и защиты информации **Уметь:** решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности **Владеть:** нормативно-правовой базой и стандартами информационной безопасности при решении стандартных задач в профессиональной деятельности	ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Знать: процессы жизненного цикла безопасных информационных систем **Уметь:** применять методы и механизмы оценки и анализа безопасности систем информационных технологий **Владеть:** проводить оценку и анализ защищенности систем информационных технологий	ПК-7 способностью разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий
Знать: назначение и специфику стандартов в области информационной безопасности как науки, основные принципы и законы их анализа; оценочные стандарты, направленные на оценивание и классификацию информационных систем и средств защиты по требованиям безопасности **Уметь:** применять международные и профессиональные стандарты в области информационной безопасности, методологии, инструментальные и вычислительные средства **Владеть:** знаниями об отечественных и зарубежных нормативно-правовых документах и стандартах в области информационной безопасности для проектирования, разработки и оценивания защищенности системы; методами построения защищенных информационных систем	ПК-8 способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**34,25**	**34,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самостоятельное изучение разделов (перечислить);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**73,75**	**73,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Теоретические основы информационной безопасности и защиты информации. Национальная безопасность РФ	8	2		2	4
2	Понятие и виды защищаемой информации	9	2		2	5
3	Объекты и угрозы информационной безопасности	9	2		2	5
4	Основы стандартизации в области информационной безопасности	9	2		2	5
5	Правовые основы защиты информации	7	2			5
6	Режим защиты государственной тайны. Режим защиты государственных информационных систем.	14	2		2	10
7	Защита критической информационной инфраструктуры.	14	2		2	10
8	Защита персональных данных	16	2		4	10
9	Аттестация объектов информатизации по требованиям безопасности информации. Лицензирование и система сертификации средств защиты информации	22	2			20
	Итого:	108	18		16	74
	Всего:	108	18		16	74

4.2 Содержание разделов дисциплины

1 Теоретические основы информационной безопасности и защиты информации. Национальная безопасность РФ

Понятие национальной безопасности РФ. Стратегия национальной безопасности Российской Федерации. Обеспечение национальной безопасности Российской Федерации. Концепция национальной безопасности Российской Федерации. Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы

2 Понятие и виды защищаемой информации

Понятия и виды защищаемой информации по российскому законодательству. Виды информации: общедоступная информация, информация ограниченного доступа. Указ президента РФ от 6 марта 1997 г. №188, ред. Указа Президента РФ от 23.09.2005 №1111 «Перечень сведений конфиденциального характера». Тайна следствия и судопроизводства. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Интеллектуальная собственность. Персональные данные.

3 Объекты и угрозы информационной безопасности

Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации. Угрозы информационной безопасности. Модель угроз и нарушителя. Общая характеристика источников угроз. Общая характеристика уязвимостей информационной системы. Процесс определения угроз безопасности информации в информационной системе.

4 Основы стандартизации в области информационной безопасности

Основные термины и определения в области стандартизации. ФЗ №184 «О техническом регулировании». ФЗ №162 «О стандартизации в Российской Федерации».

Участники работ по стандартизации в области информационной безопасности. Функции и классификация стандартов информационной безопасности. Органы управления и обеспечения ИБ РФ. Федеральный орган исполнительной власти, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию в области стандартизации. Национальный орган по стандартизации. Технические комитеты по стандартизации. Проектные технические комитеты по стандартизации. Научные организации по стандартизации. Технический комитет по общероссийским классификаторам. Совещательные органы по стандартизации**.** Организации и другие субъекты, деятельность которых связана с работами в области стандартизации.

Общие сведения при проектировании автоматизированной системы предприятия в защищенном исполнении с учетом стандартов информационной безопасности. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения», ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения»**,** ГОСТ Р ИСО 13335«Информационная технология. Методы и средства обеспечения безопасности», 17799 «Информационная технология. Практические правила управления информационной безопасностью».

5 Правовые основы защиты информации

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. Документы в области технического регулирования и стандартизации. Система сертификации средств защиты информации. Нормативные и правовые акты Оренбургской области по защите информации. Политика по обеспечению информационной безопасности в органах исполнительной власти Оренбургской области.

6 Правовой режим защиты государственной тайны. Правовой режим защиты государственных информационных систем

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 государствен-

ной 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.

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.

7 Защита критической информационной инфраструктуры

Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ. ФЗ №187 от 26.07.2017 «О безопасности КИИ РФ». Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак. ГосСОПКА. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ). Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

8 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. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методика определения актуальных 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.

9 Аттестация объектов информатизации по требованиям безопасности информации. Лицензирование и система сертификации средств защиты 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.

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.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации	2
2	2	Понятия и виды защищаемой информации	2
3	3	Модель угроз и нарушителя	2
4	4	Виды стандартов. Организации и структуры по стандартизации в области информационной безопасности	2
5	6	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах	2
6	7	Категорирование объектов КИИ РФ	2
7	8	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных	4
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 [http://znanium.com/bookread2.php?book=405000]

2. 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. Стандарты информационной безопасности [Текст] : курс лекций: учеб. пособие / В. А. Галатенко; под ред. В. Б. Бетелина.- 2-е изд. - М. : ИНТУИТ. РУ, 2006. - 264 с. - (Основы информационных технологий). - Библиогр.: с. 256-263. - ISBN 5-9556-0053-1.

2. Стандарты информационной безопасности [Текст] : курс лекций / В. А. Галатенко; под ред. В. Б. Бетелина. - М. : Интернет-Ун-т Информ. Технологий, 2004. - 328 с. - (Основы информационных технологий). - Библиогр.: с. 315-321. - ISBN 5-9556-0007-8.

3. Бачило, И. Л. Информационное право [Текст] : учеб. для магистров / И. Л. Бачило; Ин-т государства и права Рос. акад. наук, Акад. правовой ун-т.- 3-е изд., перераб. и доп. - М. : Юрайт, 2012. - 565 с. - (Магистр). - Библиогр. в конце разд. - ISBN 978-5-9916-2099-4.

4. Бабурин, С. Н. Стратегия национальной безопасности России: теоретико-методологические аспекты [Текст] : [монография] / С. Н. Бабурин, М. И. Дзлиев, А. Д. Урсул; Рос. гос. торгово-экон. ун-т. - Москва : Магистр : ИНФРА-М, 2014. - 512 с. - Прил.: с. 467-511. - Библиогр. в подстроч. примеч. - ISBN 978-5-9776-0224-2. - ISBN 978-5-16-005454-4.

5.3 Периодические издания

1. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР
2. Вестник УрФО Безопасность в информационной сфере : журнал. - Челябинск :ЮУрГУ, 2011.

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://openedu.ru/course/ITMOUniversity/INTPRO/- «Открытое образование». Курсы, МООК: Правовые основы защиты интеллектуальной собственности.

5.5 Программно-аппаратное 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.

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.