Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.Б.30 Организационное и правовое обеспечение информационной безопасности»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

Разработка защищенного программного обеспечения
(наименование направленности (профиля) образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 3 от "14" декабря 2017 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 специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В.Влацкая *расшифровка подписи*

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

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

№ регистрации 59307

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 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.7 Право, С.1.Б.19 Информатика, С.1.Б.28 Основы информационной безопасности*

Постреквизиты дисциплины: *С.2.Б.П.3 Преддипломная практика*

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: - знать основы управления рисками и построения моделей угроз безопасности информации; **Уметь:** - уметь решать типичные задачи, связанные с внедрением средств защиты информации; **Владеть:** - владеть методами сравнение условий различных финансовых продуктов средств защиты информации.	ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности
Знать: - правовые нормы реализации профессиональной деятельности с учетом интересов личности, общества и государства; **Уметь:** - пользоваться законодательными актами, на основе действующего законодательства принимать юридически грамотные решения;	ОК-5 способностью понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Владеть: - правовыми нормами реализации профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства	деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать: - иметь представление об основных закономерностях защиты персональных данных коллектива. **Уметь:** - использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности; **Владеть:** - культурой мышления, способностью к восприятию, анализу, обобщению информации, постановке цели и выбору путей ее достижения при организационном и правовом построении защиты деятельности предприятия	ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия
Знать: - основные положения законодательства Российской Федерации в области защиты информации, отечественные и зарубежные стандарты в области информационной безопасности; - основные отечественные и зарубежные стандарты в области компьютерной безопасности. **Уметь:** - применять стандарты в области обеспечения информационной безопасности; **Владеть:** - навыками работы с нормативными правовыми актами и стандартами.	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
Знать: - формализованные модели, методы и алгоритмы решения типовых задач безопасности компьютерных систем; - методы и средства мониторинга и ситуационного анализа обстановки безопасности компьютерных систем. **Уметь:** - разрабатывать формализованные модели, методы и алгоритмы решения типовых задач безопасности компьютерных систем в соответствии с отечественными и зарубежными стандартами; - использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении задач безопасности компьютерных систем в соответствии с отечественными и зарубежными стандартами; **Владеть:** - навыками анализа и разработки математических моделей безопасности компьютерных систем.	ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**35,25**	**35,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
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;* *- подготовка к рубежному контролю*	**72,75**	**72,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Национальная безопасность РФ	6	2	2		4
2	Правовые основы защиты информации	14	2	2		10
3	Режим защиты государственной тайны	14	2	2		10
4	Защита персональных данных	14	2	2		10
5	Защита критической информационной инфраструктуры	14	2	2		10
6	Режим защиты государственных информационных систем	14	2	2		10
7	Аттестация объектов информатизации по требованиям безопасности информации. Лицензирование и система сертификации средств защиты информации	21	4	2		15
8	Ответственность за правонарушения в области информационной безопасности	9	2	2		5
	Итого:	108	18	16		74
	Всего:	108	18	16		74

4.2 Содержание разделов дисциплины

1 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. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации.

2 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. Понятия и виды защищаемой информации по российскому законодательству. Организация службы безопасности на предприятии.

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. 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.

5 Защита критической информационной инфраструктуры

Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ. 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.

6 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.

7 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 инфор-

матизации 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.

8 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	Нормативно-методическая база в области национальной безопасности РФ. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации.	2
2	2	Структура органов власти по защите информации. Понятия и виды защищаемой информации	2
3	3	Режим защиты государственной тайны	2
4	4	Защита персональных данных. Методика определения актуальных угроз в ИСПДн. Требования к системе защиты ИСПДн.	2
5	5	Обследование критической информационной инфраструктуры в соответствии. Категорирование объектов критической информационной инфраструктуры.	2
6	6	Режим защиты государственных информационных систем. Построение системы защиты ГИС.	2
7	7	Аттестация объектов информатизации по требованиям безопасности информации. Лицензирование и система сертификации средств защиты информации	2
8	8	Ответственность за правонарушения в области информационной безопасности	2
		Итого:	16

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. Организационная защита информации: учебное пособие для вузов [Электронный ресурс] / Аверченков В. И., Рытов М. Ю. - Флинта, 2011.
3. Организационное обеспечение информационной безопасности [Текст] : учеб. для вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. - (Высшее профессиональное образование). - Библиогр.: с. 185. - ISBN 978-5-7695-4272-5.

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.