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.ДВ.3.1 Методы защиты 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 2016

1060387

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 5 от "7" декабря 2015 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* Н.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 *подпись* А.Е. Шухман *расшифровка подписи*

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

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

№ регистрации 45871

2

1 Цели и задачи освоения дисциплины

1 Цели и задачи освоения дисциплины

Цель (цели) 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 дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.16 Теория вероятностей и математическая статистика, Б.1.Б.18 Дискретная математика, Б.1.Б.22 Архитектура вычислительных систем, Б.1.Б.23 Технологии баз данных, Б.1.Б.24 Компьютерные сети, Б.1.В.ОД.8 Информационная безопасность и защита информации, Б.1.В.ОД.9 Администрирование информационных систем*

Постреквизиты дисциплины: *Отсутствуют*

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 основные понятия, концепции, результаты, задачи и методы классической теории вероятностей; математической статистики, теории функций комплексного переменного и функционального анализа. **Уметь:** владеть навыками решения задач математического анализа, алгебры, геометрии и информатики; уметь применять основные методы анализа к исследованию функций и	ОПК-1 способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
функциональных классов, уметь решать стандартные задачи алгебры и аналитической геометрии, уметь решать задачи информатики. **Владеть:** навыками решения обыкновенных дифференциальных уравнений и уравнений математической физики при построении системы безопасности; знать основные понятия теории обыкновенных дифференциальных уравнений и теории уравнений с частными производными, определения и свойства математических объектов в этих областях методологии защиты информации.	информационными технологиями
Знать: методы сбора, обработки и хранения информации, а также основные методы формирования научного знания. классификацию языков программирования, основные методы разработки программного обеспечения, стандарты оформления программной документации и причины нарушения компьютерной безопасности **Уметь:** использовать научные и методические ресурсы сети интернет для разработки программного обеспечения и программной документации с учетом требований информационной безопасности. составлять научные обзоры, рефераты и библиографии по тематике научных исследований. **Владеть:** базовыми навыками по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети. навыками системного и объектно-ориентированного программирования для решения стандартных прикладных 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: основные понятия, идеи, методы, связанные с дисциплинами фундаментальной математики, информатики, математического моделирования; краткую историю эволюции вычислительных систем; технологии программирования, основы архитектуры операционных систем; задачи и методы исследования и обеспечения качества и надежности программных компонентов. **Уметь:** систематизировать методы фундаментальной математики для построения математических моделей в элементарных прикладных задачах, описывать основные этапы построения алгоритмов; разрабатывать и отлаживать эффективные алгоритмы и программы с использованием современных технологий программирования. **Владеть:** методологией математического моделирования, навыками сбора и работы с математическими источниками информации, теоретическими основами построения алгоритмов; навыками работы с инструментами системного анализа.	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: 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; 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 систем. **Уметь:** применять стандарты в области обеспечения информационной безопасно-сти;	ПК-8 способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Владеть: навыками работы с нормативными правовыми актами и стандартами.	

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**53,25**	**53,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	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);* *- 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.)*	**162,75**	**162,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Теоретические основы информационной безопасности и методологии защиты информации	24	2		2	20
2	Законодательный уровень информационной безопасности	24	2		2	20
3	Организация жизненного цикла при разработке защищенного программного обеспечения и программных средств	24	2		2	20
4	Особенности информационной безопасности при разработке защищенных автоматизированных систем	24	2		2	20
5	Анализ международных и российских стандартов в области качества программного обеспечения	26	2		4	20
6	Требования безопасности для криптографических модулей	26	2		4	20
7	Административный уровень информационной безопасности. Управление рисками. Процедурный уро-	26	2		4	20

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	вень информационной безопасности					
8	Основные программно-технические меры	26	2		4	20
9	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности	16	2		10	4
	Итого:	216	18		34	164
	Всего:	216	18		34	164

4.2 Содержание разделов дисциплины

Раздел №1 Теоретические основы информационной безопасности и методологии защиты информации

Введение: предмет, содержание и задачи дисциплины, ее место среди других дисциплин учебного плана, формы отчетности, основная и дополнительная литература. Предмет защиты. Виды и формы представления информации. Понятие информационной безопасности и защиты информации. Основные составляющие информационную безопасность.

Место информационной безопасности в общей системе безопасности государства. Концепция информационной безопасности. Виды информационных ресурсов по категориям доступа. Особенности информации с ограниченным доступом. Виды и особенности конфиденциальной информации. Субъекты правоотношений в области информационной безопасности. Права и обязанности обладателя информации.

Понятие угрозы и ее основные свойства. Классификация угроз. Ущерб информационной безопасности. Организационные источники и каналы утечки информации. Основы теории информации. Коммуникационный процесс. Источники конфиденциальной информации. Организационные каналы утечки информации. Их классификация. Построение модели угроз и нарушителя.

Проблемы информационной безопасности, возникающие из-за информационных войн. Проблемы кибербезопасности в России.

Раздел №2 Законодательный уровень информационной безопасности

Структура и основные положения нормативных правовых актов в области информационной безопасности. Государственные стандарты, используемые в области информационной безопасности.

Понятие системы защиты информации. Принципы функционирования системы защиты информации. Правовые основы деятельности системы защиты информации. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Цели и задачи системы защиты информации. Организационная и функциональная структура государственной системы защиты информации. Концептуальные документы. Федеральные законы, определяющие систему защиты информации в России. Гражданский кодекс Российской Федерации. Налоговый кодекс Российской Федерации. Трудовой кодекс Российской Федерации. Семейный кодекс Российской Федерации. Кодекс Российской Федерации об административных правонарушениях.

Раздел №3 Организация жизненного цикла при разработке защищенного программного обеспечения и программных средств

Процессы жизненного цикла программных средств. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Проведение оценки. Руководство по проведению оценки. Образец модели оценки процессов жизненного цикла программного обеспечения. Пример модели оценки процессов жизненного цикла системы. Оценка процессов.

Критерии оценки безопасности информационных технологий. Требования к программному обеспечению. Особенности процессов обеспечения функциональной безопасности в серии стандартов ГОСТ Р ИСО/МЭК 15408. Особенности методологии обеспечения безопасности в серии стандартов ИСО/МЭК 13335. Особенности процессов разработки и документирования встроенных программных средств в стандарте ГОСТ Р 51904.

Раздел №4 Особенности информационной безопасности при разработке защищенных автоматизированных систем

Общие сведения при проектировании автоматизированной системы предприятия в защищенном исполнении с учетом стандартов информационной безопасности. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Методы и средства обеспечения безопасности», Практические правила управления информационной безопасностью».

Анализ информационных активов. Изучение технологического процесса обработки и хранения информации, физических условий и условий окружающей среды. Анализ программно-технических комплексов за-

щиты 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. Методика определения угроз безопасности информации в информационных системах, ФСТЭК. Классификация информационной системы по требованиям защиты информации. Определение требований к системе защиты информации информационной системы. Требования к системам обнаружения вторжений. Требования к средствам антивирусной защиты. Требования к средствам доверенной загрузки. Требования к средствам контроля съемных машинных носителей информации. Требования к межсетевым экранам. Требования безопасности информации, предъявляемые к операционным системам.

Определение субъектов и объектов доступа. Модели управления доступом.

Раздел №5 Анализ международных и российских стандартов в области качества программного обеспечения

Процесс обеспечения качества. Анализ стандартов в области надежности программного обеспечения. Анализ стандартов в области риска. Методы анализа и надежности риска. Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки.

Раздел №6 Требования безопасности для криптографических модулей

Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей». Основные понятия и идеи стандарта FIPS 140-2. Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация. Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность. Требования безопасности. Часть 3. Эксплуатационное окружение, управление криптографическими ключами. Требования безопасности. Часть 4. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.

Раздел №7 Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности

Основные понятия. Политика безопасности. Программа безопасности. Подготовительные этапы управления рисками. Основные этапы управления рисками. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Раздел №8 Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.

Раздел №9 Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности

Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Ролевое управление доступом.

Основные понятия. Активный аудит. Функциональные компоненты и архитектура. Цифровые сертификаты. Архитектурные аспекты. Классификация межсетевых экранов. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости и обслуживаемости.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Теоретические основы информационной безопасности и методологии защиты информации	2
2	2	Законодательный уровень информационной безопасности	2
3	3	Организация жизненного цикла при разработке защищенного программного обеспечения и программных средств	2
4	4	Особенности информационной безопасности при разработке защищенных автоматизированных систем	2
5	5	Анализ международных и российских стандартов в области качества программного обеспечения	4
6	6	Требования безопасности для криптографических модулей	4
7	7	Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности	4
8	8	Основные программно-технические меры	4
9	9	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ	10

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Теоретические основы информационной безопасности и методологии защиты информации	2
2	2	Законодательный уровень информационной безопасности	2
		защищенности. Обеспечение высокой доступности	
		Итого:	34

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.