

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.33 Комплексные системы защиты информации на предприятии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность
(код и наименование направления подготовки)

**Безопасность автоматизированных систем (информационные технологии и электронная
промышленность)**

(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2023

Рабочая программа дисциплины «Б1.Д.Б.33 Комплексные системы защиты информации на предприятии» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от 7 марта 2023 г.

Заведующий кафедрой

Кафедра вычислительной техники и защиты информации
наименование кафедры


подпись

Т.З. Аралбасов
расшифровка подписи

Исполнители:

Зав.каф. ВТиЗИ
должность


подпись

Т.З. Аралбасов
расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

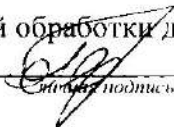
10.03.01 Информационная безопасность
код наименование

личная подпись



Т.З. Аралбасов
расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов


личная подпись

расшифровка подписи

Уполномоченный по качеству факультета


личная подпись

И.В. Крючкова
расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цели освоения дисциплины: изучение основ обеспечения безопасности автоматизированных систем.

Задачи:

1) теоретический компонент:

- освоение основ теории информационной безопасности и методологии информационной безопасности автоматизированных систем.

2) познавательный компонент:

- изучение основных положений выбора политики безопасности предприятий и организации работ по защите информации с учетом современных средств защиты и предпринимательского риска;

3) практический компонент:

- комплексное применение современных методов и средств по организации работ по защите информации на предприятии.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.10 Программно-аппаратные средства защиты информации, Б1.Д.Б.19 Методы и средства криптографической защиты информации, Б1.Д.Б.20 Техническая защита информации, Б1.Д.Б.26 Аппаратные средства вычислительной техники, Б1.Д.Б.28 Электроника и схемотехника, Б1.Д.Б.30 Защита информационных процессов в автоматизированных системах, Б1.Д.Б.32 Экономика защиты информации, Б1.Д.Б.37 Основы теории распознавания образов, Б1.Д.Б.38 Защита информации от утечки по техническим каналам, Б1.Д.В.2 Метрология и электрорадиоизмерения, Б1.Д.В.4 Лицензирование и сертификация в области защиты информации, Б1.Д.В.8 Системы охранной и пожарной сигнализации, Б1.Д.В.10 Организация работ по защите персональных данных

Постреквизиты дисциплины: Б2.П.В.П.2 Проектно-технологическая практика, Б2.П.В.П.3 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
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении	УК-8-В-1 Формирует культуру безопасного и ответственного поведения в повседневной жизни и профессиональной деятельности, обеспечивая безопасные и/или комфортные условия жизнедеятельности, труда на рабочем месте, в т.ч. с помощью средств защиты УК-8-В-2 Использует приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций и военных конфликтов	Знать: основы обеспечения техногенной и экологической безопасности автоматизированных систем. Уметь: формировать культуру безопасного и ответственного поведения в повседневной жизни и профессиональной

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
чрезвычайных ситуаций и военных конфликтов	УК-8-В-3 Идентифицирует угрозы (опасности) природного и техногенного происхождения для жизнедеятельности человека и природной среды УК-8-В-4 В случае возникновения чрезвычайных ситуаций и военных конфликтов применяет методы защиты жизнедеятельности человека, принимает участие в спасательных и неотложных аварийно-восстановительных мероприятиях	деятельности, обеспечивая безопасные и/или комфортные условия жизнедеятельности, труда на рабочем месте. Владеть: методиками идентификации угроз (опасности) природного и техногенного происхождения для жизнедеятельности человека и природной среды и средствами проведения спасательных и неотложных аварийно-восстановительных мероприятий.
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5-В-1 Использует нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций	Знать: принципы применения нормативных, правовых и методические документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности. Уметь: пользоваться нормативными, правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере информационных технологий и телекоммуникаций. Владеть: практическими навыками проведения работ по защите информации в автоматизированных системах с использованием нормативных, правовых актов, нормативных и методических документов.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6-В-1 Организует и решает задачи защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций	<u>Знать:</u> принципы реализации политики информационной безопасности автоматизированных систем в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. <u>Уметь:</u> организовывать и решать задачи защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций. <u>Владеть:</u> организационными и инженерными навыками защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению	ОПК-10-В-1 Проводит экспертизу и разработку политики безопасности, организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации в автоматизированных системах	<u>Знать: основы</u> формирования политики информационной безопасности автоматизированных систем. <u>Уметь:</u> проводить экспертизу и разработку политики безопасности, организовать и

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
информационной безопасности, управлять процессом их реализации на объекте защиты		выполнение комплекса мер по обеспечению информационной безопасности. <u>Владеть: опытом</u> управления процессом их реализации мер защиты информации на в автоматизированных системах.
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1-В-1 Организует и проводит аудит, модернизацию, разработку и внедрение систем защиты информации	<u>Знать: принципы</u> организации мероприятий по обеспечению безопасности информации в автоматизированных системах. <u>Уметь:</u> проводить аудит, модернизацию, разработку и внедрение систем защиты информации. <u>Владеть:</u> практическими навыками проведения аудита, модернизации, разработки и внедрения систем защиты информации.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	55,25	55,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	18	18
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий; - подготовка к лабораторным занятиям; - подготовка к практическим занятиям; - подготовка к рубежному контролю и т.п.)	88,75	88,75

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Ведение в дисциплину.	4	2	-	-	2
2	Принципы организации и этапы разработки КСЗИП	32	4	4	4	20
3	Кадровое обеспечение функционирования КСЗИП	34	4	4	4	22
4	Принципы и методы планирования и управления КСЗИП	40	4	6	6	24
5	Экономическая эффективность КСЗИП	34	4	4	4	22
	Итого:	144	18	18	18	90
	Всего:	144	18	18	18	90

4.2 Содержание разделов дисциплины

Раздел 1. Ведение в дисциплину.

- 1.1 Сущность и задачи комплексной защиты информации
- 1.2 Цели, задачи и принципы построения КСЗИП.
- 1.3 Требования к КСЗИП

Раздел 2. Принципы организации и этапы разработки КСЗИП

- 2.1 Разработка политики безопасности КСЗИП
- 2.2 Этапы разработки КСЗИП
- 2.3 Разработка модели КСЗИП
- 2.4 Технологическое и организационное построение КСЗИП
- 2.5 Материально-техническое и нормативно-методическое обеспечение КСЗИП

Раздел 3. Кадровое обеспечение функционирования КСЗИП

- 3.1 Специфика персонала предприятия как объекта защиты
- 3.2 Распределение функций по защите информации
- 3.3 Подбор и обучение персонала

Раздел 4 Принципы и методы планирования и управления КСЗИП

- 4.1 Задачи планирования КСЗИП
- 4.2 Виды контроля функционирования КСЗИП
- 4.3 Управление КСЗИП в условиях чрезвычайных ситуаций

Раздел 5. Экономическая эффективность КСЗИП

- 5.1 Виды ущерба от несанкционированного доступа (НСД) к информации
- 5.2 Основные методы определения затрат на информационную безопасность
- 5.3 Основные положения определения экономической эффективности защиты информации.

4.3 Лабораторные работы

№ ЛР	№ раздела	Тема	Количество часов
1	2	Лабораторная работа № 1. Модель принятия решений по выбору политики безопасности на предприятии	2

2	3	Лабораторная работа № 3. Организация защиты доступа на предприятие на основе программно-аппаратных средств «СО-БОЛЬ» и «АККОРД»	2
3	3	Лабораторная работа № 4. Защита от сетевых атак с использованием сетевых экранов и сканеров уязвимости	2
4	3	Лабораторная работа № 5. Организация систем охранной и пожарной сигнализации на предприятии	2
5	3	Лабораторная работа № 6. Построение системы видеонаблюдения на предприятии	2
6	4	Лабораторная работа № 7. Отбор персонала на предприятии	2
7	5	Лабораторная работа № 8. Распределение затрат на организацию подсистем защиты информации	2
8	5	Лабораторная работа № 9. Анализ рисков на предприятии	4
		ИТОГО:	18

4.4 Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Анализ модели угроз на предприятии	4
2	2	Анализ модели нарушителя на предприятии	4
3	3	Разработка модели комплексной защиты информации на предприятии	2
4	4	Планирование работ по защите информации на предприятии	2
5	5	Анализ экономической эффективности защиты информации на предприятии	2
6	5	Анализ рисков	4
		Итого:	12

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Болодурина, И. П. Проектирование компонентов распределенных информационных систем [Текст] : учебное пособие для магистров / И. П. Болодурина, Т. В. Волкова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : Университет, 2012. - 216 с. : ил. - Библиогр.: с. 211-215. - ISBN 978-5-4417-0077-1.

2. Соловьев, И. В. Проектирование информационных систем. Фундаментальный курс [Текст] : учеб. пособие для студентов вузов / И. В. Соловьев, А. А. Майоров ; Моск. гос. ун-т геодезии и картографии. - М. : Акад. проект, 2009. - 399 с. - (Ученое пособие для вузов). - Прил.: с. 379-393. - Библиогр.: с. 376-378. - ISBN 978-5-8291-1156-4.

5.2 Дополнительная литература

1. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2009. - 413 с. - (Высшее профессиональное образование). - Библиогр.: с. 403-406.

2. Девянин, П.Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для вузов / П.Н. Девянин. - М. : Академия, 2005. - 144 с.

3. Заботина, Н.Н. Проектирование информационных систем [Текст]: учебное пособие для студентов высших учебных заведений/ Н.Н. Заботина.-Москва: ИНФРА-М, 2013.-331 с.
4. Ретана, А. Принципы проектирования корпоративных IP-сетей = CCIE Professional Development: Advanced IP Network Design [Текст] : пер. с англ. / А. Ретана, Д. Слайс, Р. Уайт. - М. ; СПб. ; Киев : Вильямс, 2002. - 368 с. : ил. - Парал. тит. л. англ. - Пред. указ.: с. 357-367. - ISBN 5-8459-0248-7
5. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учебное пособие для вузов / А. А. Торокин . - М. : Гелиос АРВ, 2005. - 960 с. : ил.. - Библиогр.: с. 934-949.
6. Щелоков, С.А. Проектирование распределенных информационных систем [Текст] : курс лекций учебное пособие для студентов, обучающихся по программам высшего профессионального образования по направлению подготовки 230100.68 Информатика и вычислительная техника / С. А. Щелоков, Е. Н. Чернопрудова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Оренбург : Университет, 2013. - 195 с.: ил. - ISBN 978-5-4417-0332-1. - Библиогр.: с. 194-195

5.3 Периодическая литература

Журналы:

- Программные продукты и системы : журнал. - М. : Агентство "Роспечать", 2016;
- Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР, 2015.;
- Вестник компьютерных и информационных технологий : журнал. - Москва : Агентство "Роспечать", 2019. - N 1-5.

5.4 Интернет-ресурсы

1. Ассоциация по вопросам защиты информации BISA <http://bis-expert.ru/>
2. Журнал "Information Security" <http://www.itsec.ru/articles2/allpubliks>
3. Клуб информационной безопасности <http://wiki.informationsecurity.club/doku.php/main>
4. Научный журнал «Вопросы кибербезопасности» <http://cyberrus.com/>
5. Официальный сайт ФСТЭК РОССИИ fstec.ru
6. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. <https://docinfo.ru/gost-r/gost-r-51583-2014/>
7. Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне" (в редакции, актуальной с 15 сентября 2015 г., <https://base.garant.ru/10102673/>
8. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция). https://gim1-junona.rnd.eduru.ru/media/2018/07/18/1239792338/3.5.4-lokalnye_normativnye_akt-reglamentirujushhi.pdf
9. Федеральный закон РФ "О персональных данных" (152-ФЗ) 2017. <https://base.garant.ru/12148567/>

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

1. Операционная система РЕД ОС.
2. LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Программная система для организации видео-конференц-связи Webinar.ru.
4. LMS Moodle [Электронный ресурс]: система управления курсами – URL: www.moodle.osu.ru – Режим доступа: для авторизованных пользователей.

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 лаборатория технических средств защиты информации и систем охранной и пожарной сигнализации, лаборатория периферийных средств и сетевых технологий компьютерный класс, оснащенный компьютерами с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ОГУ, стендами пожарно-охранной сигнализации, СТЕНДами SDK - 6.1; SDK - 1.1;

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

ду ОГУ.