Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

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 2026

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 № 10 от "06" 03 2026 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации _____ В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры
вычислительной техники и защиты информации _____ Т.В. Полынев
должность *подпись* *расшифровка подписи*

_____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность _____ В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
главный библиограф _____ Г.С. Гоксайтис
личная подпись *расшифровка подписи*

Уполномоченный по качеству института _____ С.Н. Мирзоева
личная подпись *расшифровка подписи*

№ регистрации _____

© Полынев Т.В., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цели освоения дисциплины: изучение основ обеспечения комплексной защиты информации на предприятии.

Задачи:

1) теоретический компонент:

- освоение основ теории информационной безопасности и методологии комплексной защиты информации на предприятии;

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	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 по-	**Знать:** основы обеспечения техногенной и экологической безопасности автоматизированных систем. **Уметь**: формировать культуру безопасного и

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	мощи, методы защиты в условиях 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	ответственного поведения в повседневной жизни и профессиональной 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-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 Организовывает 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 ОПК-6-В-2 Умеет анализировать нормативные правовые акты, нормативные и методические документы ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций с точки зрения правоприменения к конкретной автоматизированной системе	**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

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		актов, нормативных и методических документов.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10-В-1 Проводит экспертизу и разработку политики безопасности , организует и поддерживает выполнение комплекса мер по обеспечение информационной безопасности, управляет процессом их реализации в автоматизированных системах	**Знать:** 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. **Уметь:** 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. **Владеть:** организационными и инженерными навыками защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами.
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 ОПК-4.1-В-2 Знает основные виды организационных мероприятий для обеспечения информационной безопасности автоматизированных систем	**Знать:** основы формирования политики информационной безопасности автоматизированных систем. **Уметь:** проводить

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		экспертизу и разработку политики безопасности , организовать и выполнение комплекса мер по обеспечение информационной безопасности. **Владеть:** методикой управления процессом реализации мер защиты информации в автоматизированных системах.

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: *- индивидуальное творческое задание (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**88,75**	**88,75**
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.	18	4	4		10
2	Построение центра мониторинга	79	8	4	18	45

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	информационной безопасности на предприятии					
3	Результативная кибербезопасность	19	4	6		15
4	Повышение осведомленности сотрудников в сфере информационной безопасности	28	2	4		20
	Итого:	144	18	18	18	90
	Всего:	144	18	18	18	90

4.2 Содержание разделов дисциплины

Раздел 1. Введение в дисциплину

1.1 Регуляторика в области информационной безопасности.

1.2 Модель жизненного цикла кибератак.

1.3 Моделирование угроз. Банк данных угроз ФСТЭК.

Раздел 2. Построение центра мониторинга информационной безопасности на предприятии

2.1 Построение процесса управления уязвимостями информационных активов на предприятии

2.2 Управление событиями информационной безопасности (SIEM)

2.3 Безопасность конечных устройств на предприятии

2.4 Организация центра мониторинга кибербезопасности на предприятии (SOC). Сервисы и функции. Управление персоналом.

Раздел 3. Результативная кибербезопасность

3.1 Результативная кибербезопасность. Основные подходы. Концепция недопустимых событий

3.2 Основные этапы кибертрансформации на предприятии в рамках концепции результативной кибербезопасности.

3.3 Методы подтверждения киберустойчивости на предприятии

Раздел 4. Повышение осведомленности сотрудников в сфере информационной безопасности.

4.1 Способы повышения осведомленности сотрудников в области информационной безопасности.

4.2 Проведение киберучений на предприятии

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Использование встроенных средств защиты информации в отечественных сертифицированных операционных системах	4
2	2	Использование Open Source решений для управления событиями информационной безопасности на предприятии	6
3	2	Использование средств криптографической защиты и электронной подписи на предприятии	4
4	2	Организация удаленного доступа к информационной инфраструктуре на предприятии	4
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Разработка модели угроз и модели нарушителя	4
2	2	Использование Open Source решений в области информационной безопасности на предприятии	8
3	4	Повышение осведомленности сотрудников в сфере информационной безопасности	6
		Итого:	18

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Болодурина, И.П. Проектирование компонентов распределенных информационных систем: учебное пособие [Электронный ресурс] /Болодурина И.П., Волкова Т.В.-ОГУ, 2012.

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 крартографии . - 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 лекцийучебное 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_akty-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. Пакет офисных приложений «МойОфис Образование»

3. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle» (http://moodle.osu.ru).

4. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

5. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. Режим доступа: http://garant.net.osu.ru.

6. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2026].

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.

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