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.В.11 Комплексная защита информации в распределенных автоматизированных системах»

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

2240906

Рабочая программа дисциплины «*Б1.Д.В.11 Комплексная защита информации в распределенных автоматизированных системах*» 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*

Исполнитель:
Доцент кафедры ВТиЗИ _____ А.Л. Коннов
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
_____ С.А. Бижигитова
личная подпись *расшифровка подписи*

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

№ регистрации _____

© Коннов А.Л., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Изучение основ обеспечения комплексной защиты информации в распределенных автоматизированных системах.

Задачи:

- изучить классификации средств защиты информации в распределенных автоматизированных системах, инструментальных программных и аппаратных средств анализа и защищенности;
- сформировать умения в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, выполняемых с использованием современных программных, программно-аппаратных и аппаратных СЗИ
- овладеть навыками разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.В.1 Прикладная теория алгоритмов и математической логики в вычислительной технике*

Постреквизиты дисциплины: *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-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием	**Знать:** философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач, основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте **Уметь:** осуществлять критический анализ и синтез информации, полученной из разных источников, формулировать и аргументировать выводы и суждения, в том числе с применением философского

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	понятийного аппарата **Владеть:** методами сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач, способностью формулировать собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий
ПК*-1 Способен диагностировать системы защиты автоматизированных систем	ПК*-1-В-1 Применяет современные методы и средства диагностирования автоматизированных систем ПК*-1-В-2 Знает порядок проведения и требования к проверкам работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации ПК*-1-В-3 Владеет навыками проверки работоспособности и эффективности применяемых средств защиты информации в автоматизированных системах	**Знать:** порядок проведения и требования к проверкам работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации в автоматизированных системах **Уметь:** проводить проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации в автоматизированных системах **Владеть:** владеть навыками проверки работоспособности и эффективности применяемых средств защиты информации в автоматизированных системах
ПК*-2 Способен администрировать системы защиты автоматизированных систем	ПК*-2-В-1 Решает задачи администрирования автоматизированных систем ПК*-2-В-2 Владеет навыками использования программных средств для автоматизации задач администрирования информационных систем	**Знать:** основы технологий, программные средства системного и прикладного назначения, устройства и принципы функционирования автоматизированных систем и основные проблемы обеспечения защиты информации и защищенности их инфраструктуры **Уметь:** администрировать и управлять

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		работой автоматизированных систем, применять меры по защите информации в автоматизированных системах **Владеть:** методиками управления работой и подходами по защите информации в автоматизированных системах с использованием программных средства системного и прикладного назначения, в том числе отечественного производства
ПК*-3 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК*-3-В-2 Знает теорию управления внештатными ситуациями и инцидентами в автоматизированных системах ПК*-3-В-3 Осуществляет обнаружение неисправностей в работе системы защиты информации автоматизированной системы	**Знать:** теорию управления внештатными ситуациями и инцидентами в автоматизированных системах **Уметь:** обнаруживать неисправности в работе системы защиты информации автоматизированной системы **Владеть:** навыками обеспечения работоспособности систем защиты информации при возникновении нештатных ситуаций
ПК*-6 Способен устанавливать и настраивать средства защиты информации в автоматизированных системах	ПК*-6-В-1 Планирует порядок и осуществляет необходимые работы по установке и настройке аппаратно-программных средств защиты ПК*-6-В-2 Знает принципы работы и характеристики основных видов средств защиты информации в автоматизированных системах	**Знать:** принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации **Уметь:** использовать программные, программно-аппаратные и технические средства для защиты информации в автоматизированных системах **Владеть:** методами установки и настройки программных, программно-аппаратных и технических средств защиты информации в автоматизированных системах

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**49,5**	**49,5**
Лекции (Л)	18	18
Практические занятия (ПЗ)	12	12
Лабораторные работы (ЛР)	18	18
Индивидуальная работа и инновационные формы учебных занятий	1	1
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа: *- выполнение курсовой работы (КР);* *- 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.*	**58,5** +	**58,5**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Понятие РАС. Общие принципы обеспечения безопасности РАС. Сетевые угрозы	12	2	2		15
2	Защита устройств	30	4	4	4	15
3	Комплексная защита РАС	50	10	4	14	15
4	Управление безопасной РАС	16	2	2		15
	Итого:	108	18	12	18	60
	Всего:	108	18	12	18	60

4.2 Содержание разделов дисциплины

№ 1 Понятие РАС. Общие принципы обеспечения безопасности РАС. Сетевые угрозы.

Понятие РАС. Безопасность оконечных устройств. Компоненты AAA, локальная и серверная аутентификация. Угрозы безопасности на канальном уровне. Категории атак на коммутаторы. Текущий уровень кибербезопасности. Злоумышленники, инструменты злоумышленников. Типы атак. Типы вредоносного ПО. Атаки доступа. Атаки методами социальной инженерии. DoS- и DDoS-атаки. Уязвимости IP и угрозы. Уязвимости TCP и UDP

№2 Защита устройств.

Защита пограничного маршрутизатора. Мониторинг и управление устройствами. Функция отказоустойчивой конфигурации РАС. Виртуальные частные сети. Безопасное управление и отчетность. Уязвимости плоскости контроля и плоскости управления. Списки контроля доступа.

№3 Комплексная защита РАС.

Технологии межсетевых экранов. Типы межсетевых экранов. Классический брандмауэр. ZPF. Системы обнаружения вторжений, системы предотвращения вторжений. Сигнатуры IPS: триггеры, действия. Безопасность конечной точки. Технологии Advanced Malware Protection (AMP), Email Security Appliance (ESA), Web Security Appliance (WSA), Network Admission Control (NAC). Технологии IPsec. Cisco Adaptive Security Appliance (ASA): режимы работы, уровни безопасности, развертывание, политики обслуживания.

№ 4 Управление безопасной PAC

Безопасность эксплуатации PAC. Тестирование безопасности PAC. Типы сетевых тестов. Инструменты для тестирования PAC. Понятие политики безопасности PAC. Иерархия политик безопасности. Обеспечение безопасности канального уровня. Виды атак на коммутатор, методы защиты от них. Обучение пользователей безопасной работе в PAC. Реагирование на нарушение безопасности.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Технология транслирования адресов. Настройка статического и динамического NAT	2
2	2	Настройка списков контроля доступа ACL	2
3	3	Настройка брандмауэра ZPF	2
4	3	Настройка системы предотвращения вторжений IPS	4
5	3	Настройка туннеля IPSec VPN	4
6	3	Работа с межсетевым экраном ASA	4
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Компоненты аутентификации AAA	2
2	2	Понятие отказоустойчивости PAC. Протокол отказоустойчивости HSRP	2
3	2	Настройка VLAN	2
4	3	Анализ сетевого трафика	2
5	3	Инвентаризация аппаратно-программных средств вычислительной системы	2
6	4	Защита устройств на канальном уровне	2
		Итого:	12

4.5 Курсовая работа (8 семестр)

Тема курсовой работы: Аудит безопасности сети предприятия

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Гультяева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 26.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

2. Болодурина, И. П. Проектирование компонентов распределенных информационных систем [Текст] : учеб. 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.

3. 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. - Библиогр.: с. 194-195. - ISBN 978-5-4417-0332-1.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2014. - 416 с. : ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

5.2 Дополнительная литература

1. Шевченко, В. П. Вычислительные системы, сети и телекоммуникации [Текст] : учеб. для вузов / В. П. Шевченко; Моск. авиац. ин-т (Нац. исслед. ун-т). - М. : КноРус, 2012. - 288 с. : ил. - Библиогр.: с. 287-288. - ISBN 978-5406-00521-7.

2. Васильков, А. В. Безопасность и управление доступом в информационных системах [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / А. В. Васильков, И. А. Васильков. - Москва : Форум : ИНФРА-М, 2014. - 368 с. : ил. - (Профессиональное образование). - Библиогр.: с. 356-358. - Предм. указ.: с. 359-363. - ISBN 978-5-91134-360-6. - ISBN 978-5-16-006736-0.

5.3 Периодические издания

1. Защита информации. Инсайд. 2020-2026.

5.4 Интернет-ресурсы

1. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование», Каталог курсов, МООК: «Защита информации»
2. https://academy.yandex.ru/schools/shkib - «Академия Яндекса», Школы: «Школа информационной безопасности»
3. https://mooc.enu.kz/course/view.php?id=383 - Eurasian Online Course Platform, Массовые открытые онлайн-курсы, Курс: «Безопасность вычислительных сетей»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru.

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 компьютерами с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ОГУ и лаборатория периферийных средств и сетевых технологий. Используется оборудование: Стойка 19"; коммутатор D-Link DES-1100-26; коммутатор D-Link DES-3526; коммутатор D-Link DFL-260E; коммутатор Cisco <SRW208MP-K9-EU>SF302-08MP; экран межсетевой Cisco ASA5505-K8; "Глонасс-GPS"- модуль типа "SIM908"; модуль беспроводной связи Xbee; антенна РЭМО ВОЛНА-digital; антенна АШ-433(М).

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