

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.30 Защита информационных процессов в 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 2025

Рабочая программа дисциплины «Б1.Д.Б.30 Защита информационных процессов в автоматизированных системах» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от "22" 02 2025г.

Заведующий кафедрой

Кафедра вычислительной техники и защиты информации  В.В. Тугов
наименование кафедры подпись расшифровка подписи

Исполнители:

Старший преподаватель кафедры ВТ и ЗИ  Т.В. Абрамова
должность подпись расшифровка подписи

должность подпись расшифровка подписи

СОГЛАСОВАНО:

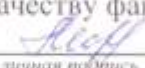
Председатель методической комиссии по направлению подготовки

10.03.01 Информационная безопасность  В.В. Тугов
код наименование личная подпись расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов

 С.А. Биктимирова
личная подпись расшифровка подписи

Уполномоченный по качеству факультета

 С.Н. Морозова
личная подпись расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование у студентов знаний и умений по защите информационных процессов в автоматизированных системах с использованием современных организационно-правовых, инженерно-технических, программно-аппаратных и криптографических методов и средств в области выбранного профиля подготовки – «Безопасность автоматизированных систем».

Задачи:

- 1) *теоретический компонент:*
 - освоение теоретических основ защиты информационных процессов в автоматизированных системах: концепций защиты технологических процессов обработки данных в автоматизированных системах различной архитектуры, а также моделей построения систем защиты;
- 2) *познавательный компонент:*
 - изучение основных руководящих документов, политик безопасности, а также - базовых методов и средств комплексной защиты информационных процессов в автоматизированных системах;
- 3) *практический компонент:*
 - применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при построении и администрировании систем защиты информационных процессов в автоматизированных системах.

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.18 Теория информации, Б1.Д.Б.20 Техническая защита информации, Б1.Д.Б.21 Введение в специальность, Б1.Д.Б.25 Технологии и методы программирования, Б1.Д.Б.29 Информационные технологии, Б1.Д.Б.37 Основы теории распознавания образов*

Постреквизиты дисциплины: *Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.34 Проектирование систем информационной безопасности, Б1.Д.В.Э.6.2 Проектирование локальных вычислительных сетей*

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-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта	Знать: необходимые для осуществления профессиональной деятельности правовые нормы и основные методы оценки разных способов решения профессиональных задач Уметь: анализировать альтернативные варианты решений для достижения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. Владеть: методиками постановки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах
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 обеспечению информационной безопасности, управляет процессом их реализации в автоматизированных системах	Знать: программно-аппаратные средства защиты информации в автоматизированных системах, типовых операционных системах, системах управления базами данных, компьютерных сетях Уметь: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности Владеть: принципами формирования политики информационной безопасности объекта информатизации
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3-В-1 Планирует порядок и осуществляет необходимые работы по установке, настройке, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ОПК-4.3-В-3 Понимает принципы устройства и функционирования программных, программно-аппаратных и технических средств защиты информации	Знать: требования по установке, настройке, администрированию и обслуживанию программно-аппаратных и технических средств защиты информации в автоматизированных системах Уметь: настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз информационной

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		безопасности Владеть: навыками планирования и организации работы персонала автоматизированной системы с учетом требований по защите информации
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4-В-1 Применяет современные методы и средства диагностирования и мониторинга автоматизированных систем ОПК-4.4-В-2 Выбирает необходимые инструментальные средства для анализа защищенности автоматизированных систем	Знать: критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: контролировать уровень защищённости в автоматизированных системах, регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах Владеть: навыками проведения аудита защищённости 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	
	5 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	86,5	86,5
Лекции (Л)	34	34
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
Консультации	1	1

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
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.	57,5 +	57,5
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Раздел 1. Введение в дисциплину. Характеристика информационных систем и информационных процессов	14	4	2	4	4
2	Раздел 2. Основы принципы защиты информационных процессов в автоматизированных системах	46	16	2	2	18
3	Раздел 3. Стандарты по защите информации и информационных процессов	28	4	2	2	18
4	Раздел 4. Организация и средства защиты информационных процессов в автоматизированных системах	56	10	10	26	20
	Итого:	144	34	16	34	60
	Всего:	144	34	16	34	60

4.2 Содержание разделов дисциплины

Раздел 1. Введение в дисциплину. Характеристика информационных систем и информационных процессов

1.1 Общая характеристика информационных систем и информационных процессов (ИП) как объектов защиты.

1.2. Государственные стандарты на разработку и создание информационных систем и автоматизированных систем в защищенном исполнении.

Раздел 2. Основы принципы защиты информационных процессов в автоматизированных системах

2.1. Основные угрозы информации в автоматизированных системах; специфика возникновения угроз в открытых сетях; особенности защиты информации на узлах компьютерной сети; системные вопросы защиты программ и данных.

2.2 Анализ рисков.

2.3 Модель угроз и модель нарушителя безопасности информации в автоматизированных системах.

2.4. Политика информационной безопасности для автоматизированных систем.

- 2.5. Государственная политика в области безопасности ИП в автоматизированных системах.
- 2.6. Требования к программной и программно-аппаратной реализации средств защиты ИП.
- 2.7. Система лицензирования и сертификации средств защиты ИП. Аттестация защищенных систем. Структуры в РФ, обеспечивающие лицензирование и сертификацию.
- 2.8. Нормативная база и ответственность за нарушения в области защиты автоматизированных системах.

Раздел 3. Стандарты по защите информации и информационных процессов

- 3.1. Стандарт США «Оранжевая книга». Европейские стандарты по безопасности АС. Критерии оценки защищенности ИП. Функциональные требования. Вопросы гарантий и эффективности.
- 3.2 Отечественные стандарты в области защиты ИП в АС.

Раздел 4. Организация и средства защиты информационных процессов в автоматизированных системах

- 4.1 Базовые концепции безопасности ИП в автоматизированных системах. Профиль защиты.
- 4.2. Подсистемы управления доступом, регистрации и учета, контроля целостности, антивирусной, сетевой и криптографической защиты информации в автоматизированных системах.
- 4.3. Гарантии безопасности ИП в автоматизированных системах. Уровни гарантий. Методология анализа гарантий.
- 4.4 Аппаратно-программные и криптографические средства защиты ИП в АС.
- 4.5. Каналы утечки информации. Средства защиты информации от утечек по техническим каналам.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Построение учебной локальной сети на базе УИСС в защищенном исполнении	2
2	1	Построение учебной беспроводной сети в защищенном исполнении	2
3	2	Выявление аномальной сетевой активности на основе анализа сетевого трафика	2
4	3	Обеспечение информационной безопасности учебной локальной сети на базе УИСС посредством межсетевого экранирования	2
5	4	Изучение методов защиты автоматизированных систем от сетевых атак на примере атаки ping flooding на базе УИСС	2
6	4	Изучение систем защиты от НСД на примере ПАК Аккорд и ШИПКА	2
7	4	Исследование уязвимостей ПК программным средством XSpider 7.7	2
8	2, 3, 4	Методы и средства защиты информационных процессов в автоматизированных системах	20
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Построение учебной локальной сети на базе УИСС в защищенном исполнении	2
2	1	Обеспечение информационной безопасности учебной локальной сети на базе УИСС посредством межсетевого экранирования	2
3	2	Построение учебной беспроводной сети в защищенном	2

№ занятия	№ раздела	Тема	Кол-во часов
		исполнении	
4	3	Выявление аномальной сетевой активности на основе анализа сетевого трафика	2
5	4	Изучение методов защиты автоматизированных систем от сетевых атак на примере атаки ping flooding на базе УИСС	2
6	4	Изучение систем защиты от НСД на примере ПАК Аккорд и ШИПКА	2
7	4	Исследование уязвимостей ПК программным средством XSpider 7.7	2
8	2, 3, 4	Исследование методов и средств защиты информационных процессов в автоматизированных системах	2
		Итого:	16

4.5 Курсовая работа (5 семестр)

Примерные темы курсовой работы

- 1 Сравнительный анализ программно-аппаратных средств защиты информации от несанкционированного доступа.
- 2 Исследование методов противодействия сниффингу.
- 3 Анализ защищенности дисков при использовании программы VipNet SafeDisk.
- 4 Сравнительный анализ информационной безопасности ОС Windows и ОС Linux.
- 5 Исследование уязвимостей ОС с использованием программного средства Microsoft Baseline Security Analyzer.
- 6 Исследование уязвимостей компьютерной системы, защищаемой средствами Secret Net.
- 7 Сравнительный анализ программных сканеров уязвимостей информационной системы.
- 8 Анализ методов защиты информации от несанкционированного копирования.
- 9 Исследование методов мониторинга сетевого трафика.
- 10 Исследование методов мониторинга систем защиты информации в компьютерных сетях.
- 11 Анализ методов противодействия DOS и DDos-атакам.
- 12 Анализ методов обнаружения аномалий в сетевом трафике автоматизированных систем.
- 13 Исследование интеллектуальных методов обнаружения аномалий в сетевом трафике АС.
- 14 Исследование методов резервирования каналов связи в автоматизированных системах.
- 15 Исследование методов защиты доступа к мобильным объектам информатизации (на примере квадрокоптера).
- 16 Анализ уязвимостей сетевых протоколов стека TCP/IP.
- 17 Сравнительный анализ защищенности сетевых протоколов.
- 18 Анализ эффективности средств защиты информации в беспроводных сетях.
- 19 Исследование методов защиты информации с использованием защищенных сетевых протоколов.
- 20 Сравнительный анализ программных средств обнаружения вторжений (IDS-систем).
- 21 Сравнительный анализ программных средств обнаружения утечек (DLP-систем).
- 22 Анализ методов контроля поведения пользователей в автоматизированных системах.
- 23 Анализ эффективности программы контроля и обнаружения вторжений Snort.
- 24 Сравнительный анализ эффективности программно-аппаратных средств Аккорд и Соболев.
- 25 Анализ программ удаленного управления компьютером.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 **Малюк, А. А. Введение в защиту информации в автоматизированных системах** [Текст] : учеб. пособие для студентов, обучающихся по спец., не входящим в группу спец. в обл. информ. безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин.- 2-е изд. - М. : Горячая линия-Телеком, 2004. - 147 с.

2 **Галатенко, В. А. 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.

5.2 Дополнительная литература

1 **Технические каналы утечки информации и средства защиты информации от утечек по техническим каналам** [Электронный ресурс] : электронный курс лекций / А. Г. Африн, Т. В. Абрамова, Н. М. Бардукова, И. И. Каскинов, К. А. Ковальский; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2014. - 8 с.

Режим доступа:

http://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=980

2 **Девянин, П. Н. Модели безопасности компьютерных систем** [Текст] : учеб. пособие для вузов / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование : информационная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1

3 **Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства** [Текст] : учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. : ил. - Библиогр.: с. 524-529. - Предм. указ.: с. 530-542. - ISBN 5-94074-383-8.

5.3 Периодические издания

Журналы:

- Вестник компьютерных и информационных технологий: журнал. - Москва: Агентство "Роспечать", 2024. - Т. 20, N 1-6 [1 эр];
- Информационные технологии: журнал // Информационные технологии с ежемесячным приложением. - Москва: Агентство "Роспечать", 2024. - Т. 29, N 1-6 [1 эр].
- Защита информации. Инсайд : журнал. - Москва : ИД "Афина", 2023. - N 1-3 [1 эр]

5.4 Интернет-ресурсы

1. Портал по тематике информационной безопасности: <http://www.securitylab.ru/>
2. Сайт ассоциации по вопросам защиты информации BISA: <http://bis-expert.ru/>
3. Сайт Федеральной службы по техническому и экспортному контролю: <https://fstec.ru/>

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений LibreOffice.
3. Платформа для проведения онлайн мероприятий и видеоконференций «DION».

4. Яндекс.Браузер - браузер, созданный компанией «Яндекс» на основе движка (бесплатная версия). Режим доступа: <https://browser.yandex.ru>.

6. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2025].

7. <http://edu.garant.ru/garant/study/> - Интернет-версия ГАРАНТ-Образование, Система ГАРАНТ для студентов, аспирантов и преподавателей.

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.

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