Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.8 Основы управления информационной безопасностью»

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 2021

Рабочая программа дисциплины *«Б1.Д.Б.8 Основы управления информационной безопасностью»* рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 9 от "16" апреля 2021 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации _____ Т.З. Аралбаев
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ВТиЗИ _____ Р.Р. Галимов
должность *подпись* *расшифровка подписи*

_____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность _____ Т.З. Аралбаев
код, наименование *личная подпись* *расшифровка подписи*

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

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

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование знаний по основам теории и практики управления информационной безопасностью на предприятиях и в организациях.

Задачи:

- освоение основ теории управления информационной безопасностью: концепциями контроля и оптимизации стратегии и тактики защиты объектов информатизации с учетом специфики организации и видов угроз;
- изучение основных положений разработки методологии управления организацией и реализацией политик информационной безопасности на предприятиях, знакомство с базовыми методами и средствами управления комплексной защитой объектов информатизации;
- применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств управления информационной безопасностью в научно-исследовательских и практических разработках, а также при эксплуатации систем защиты информации.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.12 Право, Б1.Д.Б.16 Основы экономики и финансовой грамотности*

Постреквизиты дисциплины: *Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности*

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 компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с	**Знать:** - основную теорию сбора и анализа информации о защищенности информационной системы предприятия с использованием компьютерных технологий. **Уметь:** - осуществлять анализ угроз информационной безопасности автоматизированной системы (АС); **Владеть:**- навыками разработки политики ИБ АС и модернизации системы защиты информации.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	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	
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 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	**Знать:**- основы теории проектирования систем защиты информации АС с с учетом нормативно-правовых документов. **Уметь:** оценивать риски ИБ АС. **Владеть:** навыками разработки проекта системы защиты АС.
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6-В-1 Понимает важность планирования целей собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда УК-6-В-2 Реализует намеченные цели с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда УК-6-В-3 Демонстрирует интерес к учебе и использует предоставляемые возможности для приобретения новых знаний и навыков УК-6-В-4 Критически оценивает эффективность использования времени при решении поставленных задач	УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие	ОПК-5-В-1 Использует нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	**Знать:**- основные нормативные правовые акты, определяющие вопросы построения и

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
деятельность по защите информации в сфере профессиональной деятельности	информационных технологий и телекоммуникаций	эксплуатации систем управления ИБ. **Уметь:**- анализировать нормативно-правовые акты с точки зрения правоприменения к конкретной АС. **Владеть:**- навыками модернизации системы защиты и приведения параметров АС к требованиям нормативно правовых актов.
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	**Знать:**- основные нормативные правовые акты ФСБ и ФСТЭК РФ, определяющие вопросы построения и эксплуатации систем управления ИБ. **Уметь:**- анализировать нормативно-правовые акты ФСБ и ФСТЭК РФ с точки зрения правоприменения к конкретной АС. **Владеть:**- навыками модернизации системы защиты и приведения параметров АС к требованиям нормативно правовых актов.
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:**- знать принципы разработки политики ИБ. **Уметь:** - создавать прототипы документов политики ИБ. **Владеть:** - навыками применения комплексного подхода к обеспечению ИБ.
ОПК-4.2 Способен администрировать операционные системы, системы управления базами	ОПК-4.2-В-1 Осуществляет мониторинг, администрирование операционных систем, систем управления базами данных и вычислительных сетей	**Знать:**основные виды угроз операционных систем, систем управления БД, вычислительных сетей.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
данных, вычислительные сети		**Уметь:** осуществлять поиск и анализ уязвимостей операционных систем, систем управления БД, вычислительных сетей. **Владеть:**- навыками контроля журналов событий операционных систем, систем управления БД, вычислительных сетей.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**84,25**	**84,25**
Лекции (Л)	34	34
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
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.*	**23,75**	**23,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основы управления информационной безопасностью	20	6	6	2	6

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
2	Система менеджмента информационной безопасности. Система менеджмента информационной безопасности. Основные нормативные документы и стандарты в области управления ИБ	30	8	6	10	6
3	Политика информационной безопасности	30	8	4	12	6
4	Администрирование компьютерных систем и вычислительных систем	20	12	-	10	6
	Итого:	108	34	16	34	24
	Всего:	108	34	16	34	24

4.2 Содержание разделов дисциплины

№ 1 Основы управления информационной безопасностью. *Содержание раздела*

Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности. Производственные требования к управлению доступом к системам. Документированная политика управления доступом к информации. Управление доступом пользователей. Управление привилегиями. Управление пользовательскими паролями. Управление доступом к сети. Управление сетевой маршрутизацией. Управление доступом к компьютерам. Система управления паролями. Управление доступом к приложениям.

№ 2 Система менеджмента информационной безопасности. Основные нормативные документы и стандарты в области управления ИБ. Преимущества системного подхода к управлению рисками. Структура документации по управлению рисками. Структура системы управления рисками. Непрерывная деятельность по управлению рисками. Оценка рисков ИБ. Обработка рисков ИБ.

№ 3 Политика информационной безопасности.

Политика информационной безопасности. Координация действий по защите информации. Распределение обязанностей по обеспечению информационной безопасности.

№ 4 Администрирование компьютерных систем и вычислительных систем

Операционные процедуры и обязанности. Процедуры реагирования на события. Разделение обязанностей. Сетевое администрирование. Средства управления безопасностью сетей. Active Directory. Групповые политики безопасности.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Анализ уязвимостей компьютерной системы с использованием программных средств	2
2	2	Создание контроллера домена на базе Windows Server 2008	2
3	2	Оснастки Active Directory	2
4	2	Создание объектов Active Directory	6
5	3	Делегирование и безопасность объектов Active Directory	4
6	3	Автоматизация создания учетных записей пользователей	4
7	3	Создание групп и управление ими	4
8	4	Реализация групповой политики	2
9	4	Настройка области действия групповой политики	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
10	4	Делегирование членства с помощью групповой политики	2
11	4	Управление параметрами безопасности	2
12	4	Конфигурация параметров аудита	2
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1,2	Инвентаризация информационных активов организации	2
2	1,2	Модель нарушителя	2
3	1,2	Модель актуальных угроз	4
4	1,2	Оценка рисков АС организации	4
5	3	Прототип документа политики ИБ	4
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 11.04.2023). – Библиогр. в кн. – ISBN 978-5-238-03200-9. – Текст : электронный..

2 Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие : [16+] / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612591 (дата обращения: 11.04.2023). – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный.

5.2 Дополнительная литература

1. Галимов, Р. Р. Управление информационной безопасностью [Электронный ресурс] : методические указания для студентов, обучающихся по программам высшего образования по направлению подготовки 10.03.01 Информационная безопасность / Р. Р. Галимов, Е. И. Ряполова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т", Каф. вычисл. техники и защиты информ. - Электрон. текстовые дан. (1 файл: 2.48 Мб). - Оренбург : ОГУ, 2016. - 88 с. - Режим доступа: http://artlib.osu.ru/web/books/metod_all/10317_20160517.pdf.

2. Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 11.04.2023). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный..

5.3 Периодические издания

1. Информация и безопасность : журнал. - Москва : Агентство "Роспечать", 2010, 2013.
2. Управление риском : журнал. - Москва : Агентство "Роспечать",

5.4 Интернет-ресурсы

http://www.xakep.ru/ -«Журнал хакер»

http://www.intuit.ru - Национальный Открытый Университет "ИНТУИТ".

http://www.fstec.ru Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

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

1. Пакет офисных приложений LibreOffice.

2. Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа \\fileserver1\GarantClient\garant.exe в локальной сети ОГУ.

3. Операционная система РЕД ОС.

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.

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