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.18 Основы информационной безопасности»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Вычислительные машины, комплексы, системы и сети
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2026

Рабочая программа дисциплины *«Б1.Д.Б.18 Основы информационной безопасности»* 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
09.03.01 Информатика и вычислительная техника _____ В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

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

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

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование знаний об основных составляющих информационной безопасности государства, общества и личности; умений и навыков использования организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при решении стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.

Задачи:

1) теоретический компонент:

– освоение основ теории информационной безопасности, знакомство с современными задачами, научной терминологией, моделями и концепциями защиты прав на информатизацию государства, общества и личности и построения систем информационной безопасности;

2) познавательный компонент:

– изучение основных положений стратегии информационной войны; основных видов обеспечения систем информационной безопасности, методов оценки уровня защищенности компьютерных систем, методов и средств комплексной защиты объектов информатизации;

3) практический компонент:

– применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств информационной безопасности в научно-исследовательских и практических разработках в области информатики и вычислительной техники.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика*

Постреквизиты дисциплины: *Б1.Д.В.10 Методы и средства защиты компьютерной информации, Б1.Д.В.15 Безопасность информационных систем и баз данных*

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
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3-В-1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3-В-2 Умеет решать стандартные задачи профессиональной	**Знать:** основы информационной и библиографической культуры; основные требования информационной безопасности при решении стандартных задач профессиональной деятельности; методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности **Уметь:** формулировать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности; применять информационно-коммуникационные технологии для решения стандартных задач профессиональной

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	деятельности с учетом требований информационной безопасности **Владеть:** методами поиска и анализа информации в профессионально-практической деятельности на основе информационной и библиографической культуры с учетом соблюдения авторского права и основных требований информационной безопасности

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	3 семестр	всего
Общая трудоёмкость	**180**	**180**
Контактная работа:	**50,25**	**50,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- индивидуальное творческое задание;* *- 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)*	**129,75**	**129,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 3 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в дисциплину	14	2	2		10
2	Защита информации на конечных устройствах	64	4	2	8	50
3	Защита информации в корпоративной сети	90	10	12	8	60
4	Результативная кибербезопасность	12	2			10
	Итого:	180	18	16	16	130
	Всего:	180	18	16	16	130

4.2 Содержание разделов дисциплины

Раздел 1. Введение в дисциплину

Регуляторика в области информационной безопасности. Модель жизненного цикла кибератак. Моделирование угроз.

Раздел 2. Защита информации на конечных устройствах.

Программно-аппаратные средства криптографической защиты информации. Встроенные средства защиты информации в отечественных сертифицированных операционных системах. Системы защиты конечных точек (EPP, EDR).

Раздел 3. Защита информации в корпоративной сети

Анализаторы сетевого трафика (NTA). Организация виртуальных частных сетей (VPN). Средства обнаружения и предупреждения вторжений (IDS,IPS). Защита веб-приложений (WAF). Межсетевые экраны нового поколения (NGFW). Платформы создания ложных целей, песочницы

Раздел 4. Результативная кибербезопасность

Результативная кибербезопасность. Основные подходы. Концепция недопустимых событий. Основные этапы кибертрансформации на предприятии в рамках концепции результативной кибербезопасности. Методы подтверждения киберустойчивости на предприятии. Способы повышения осведомленности сотрудников в области информационной безопасности. Проведение киберучений на предприятии

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2,3	Использование средства криптографической защиты информации CryptoPro в информационных системах предприятия	2
2	2,3	Изучение встроенных средств защиты в отечественных сертифицированных операционных системах	4
3	2,3	Организация виртуальных частных сетей (VPN) на базе OpenVPN	4
4	2,3	Построение киберполигона для моделирования корпоративной сетевой инфраструктуры	6
			16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Анализ методики ФСТЭК «Методика оценки угроз безопасности информации»	2
2	2,3	Организация органа криптографической защиты информации в организации	2
3	2,3	Организация виртуальных частных сетей на базе отечественных сертифицированных средств защиты информации и Open Source продуктов	6
4	2,3	Встроенные средства защиты отечественных сертифицированных операционных систем	4
5	2,3	Средства моделирования корпоративной сетевой инфраструктуры	2

№ занятия	№ раздела	Тема	Кол-во часов
		Итого:	16

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

2 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.

5.3 Периодические издания

– Вестник компьютерных и информационных технологий: журнал. - Москва: Агентство "Роспечать", 2023. - Т. 20, N 1-6 [1 эр];

– Защита информации. Инсайд : журнал. - Москва : ИД "Афина", 2023. - N 1-3 [1 эр]

– Информационные технологии: журнал // Информационные технологии с ежемесячным приложением. - Москва: Агентство "Роспечать", 2023. - Т. 29, N 1-6 [1 эр].

5.4 Интернет-ресурсы

1. Абрамова, Т. В. Основы информационной безопасности (09.03.01 очн.) [Электронный ресурс] : электронный учебный курс в системе Moodle / Т. В. Абрамова; Оренбург. гос. ун-т. - Оренбург : ОГУ, 2023. - 9 с. в РТО- Загл. с тит. экрана.
2. Единое окно доступа к образовательным ресурсам: информационная система. – Электрон. дан. – ФГУ ГНИИ ИТТ «Информика», 2005 – 2011; Министерство образования и науки РФ, 2005 – 2016. – Режим доступа: http://window.edu.ru/ . – Загл. с экрана.
3. Портал по тематике информационной безопасности: http://www.securitylab.ru/
4. Сайт ассоциации по вопросам защиты информации BISA: http://bis-expert.ru/
5. Сайт научного журнала «Вопросы кибербезопасности»: http://cyberrus.com/
6. 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 «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 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.