Федеральное государственное бюджетное образовательно учреждение
высшего образования
«Камчатский государственный университет имени Витуса Беринга»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (КУРСА, МОДУЛЯ)

Б1.В.ДВ.02.02 Основы информационной безопасности

38.03.04 Государственное и муниципальное управление

Форма обучения: очная

Федеральный государственный образовательный стандарт высшего образования- по направлению подготовки 38.03.04 Государственное и муниципальное управление (приказ Минобрнауки России от 13.08.2020 г. № 1016)

Петропавловск-Камчатский
2026 г.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

1.1. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.ДВ.02.02 Основы информационной безопасности относится к дисциплинам по выбору образовательной программы по направлению подготовки 38.03.04 Государственное и муниципальное управление профиль «Государственное и муниципальное управление», год набора 2025.

1.2. Цель освоения дисциплины (модуля)

Целью освоения учебной дисциплины «Основы информационной безопасности» является формирование у студентов компетенций, необходимых для использования изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.3. Планируемые результаты обучения по дисциплине (модулю)

Достижение цели освоения дисциплины (модуля) обеспечивается через формирование следующих компетенций*:*

Таблица 1

Код и наименование компетенции	**Код и наименование индикатора достижения компетенций, которые формирует дисциплина (модуль)**	**Планируемые результаты обучения**
УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.6. Осуществляет поиск необходимой информации для решения стандартных коммуникативных задач с применением ИКТ-технологий	Знает: методы и модели управления информационными ресурсами и информационными системами Умеет: определять вид программного средства для моделирования экономических и управленческих процессов; использовать передовые методы управления проектами по информатизации. Владеет: навыками и умениями для решения профессиональных задач.
ПК 8 Регулирование в сфере прохождения государственной гражданской службы (муниципальной службы)	ПК 8.2 Умеет работать в информационной системе и с базами данных по ведению, учету кадров	Знает работать с информационными системами и с базами данных по ведению, учету кадров. Умеет работать в информационной системе и с базами данных по ведению, учету кадров. Владеет навыками работы в информационной системе и с базами данных по ведению, учету кадров.

1.4. Объем дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет очно 3 з.е, 108 (академ. часов) Таблица 2

Вид учебной работы	Количество академ. часов
	Очно
4.1. Объем контактной работы обучающихся с преподавателем	48
4.1.1. аудиторная работа	
в том числе:	
лекции	16
практические занятия, семинары, в том числе практическая подготовка	32
лабораторные занятия	
4.1.2. внеаудиторная работа	
в том числе:	
индивидуальная работа обучающихся с преподавателем	
курсовое проектирование/работа	
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем	
4.2. Объем самостоятельной работы обучающихся	60
в том числе часов, выделенных на подготовку к зачету	

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Тематическое планирование дисциплины (модуля):

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад.часах		Трудоёмкость по видам учебных занятий (в акад.часах)							
				Лекции		Практ. занятия		Лаб. занятия		Сам. работа	
		Очно		Очно		Очно		Очно		Очно	
1.	**Модуль 1. Основополагающие положения информационной безопасности**										
2.	Тема 1.1. Международные стандарты информационного обмена	6		1		2				3	
3.	Тема 1.2. Понятие угрозы	6		1		2				3	
4.	Тема 1.3 Информационная безопасность в условиях функционирования в России	6		1		2				3	
5.	Тема 1.4. Понятие о видах вирусов	6		1		2				3	
6.	Тема 1.5. Три вида возможных нарушений информационной системы	6		1		2				3	
7.	Тема 1.6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	6		1		2				3	

8.	Тема 1.7. Основные положения теории информационной безопасности	6		1		2				3	
9.	Тема 1.8. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	6		1		2				3	
10.	Тема 1.9. Модели безопасности и их применение	6		1		2				3	
11.	**Модуль 2. Защита информации**										
12.	Тема 2.1. Использование защищенных компьютерных систем	6		1		2				3	
13.	Тема 2.2. Методы криптографии	6		1		2				3	
14.	Тема 2.3. Основные технологии построения защищенных систем	6		1		2				3	
15.	Тема 2.4 Место информационной безопасности экономических систем в национальной безопасности страны	6		1		2				3	
16.	Тема 2.5. Защита экономических систем	6		1		2				3	
17.	Тема 2.6. Обмен конфиденциальной информацией	6		1		2				3	
18.	Тема 2.7. Структура банковских информационных систем в области защиты информации	6		1		2				3	
19.	Тема 2.8. Важность защиты экономических систем	6		-		-				6	
20.	Тема 2.9. Концепция информационной безопасности	6		-		-				6	
	Курсовое проектирование/работа	*X*		*X*		*X*		X	X-	*X*	
	Подготовка к экзамену (зачету)	*X*		*X*		*X*		X	X-	*X*	
	Итого:	108		16		32		X	X	60	

2.2. Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание дисциплины (дидактические единицы) *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)*
1	**Модуль 1. Основополагающие положения информационной безопасности**	Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.
2	Тема 1.1. Международные стандарты информационного обмена	Международные стандарты информационного обмена. Протоколы (protocols) — это набор правил и процедур, регулирующих порядок осуществления некоторой связи.
3	Тема 1.2. Понятие угрозы	Понятие угрозы. Угроза в отношении человека в настоящее время трактуется, в первую очередь, с позиций уголовного права.

4	Тема 1.3 Информационная безопасность в условиях функционирования в России глобальных сетей	Информационная безопасность в условиях функционирования в России глобальных сетей. Главной целью создания сети Интернет было обеспечение функциональности при выходе из строя одного или нескольких ее узлов, цель в общем со-стояла в обеспечение безопасности.
5	Тема 1.4. Понятие о видах вирусов	Понятия о видах вирусов. Вирус, как программа, состоит из двух частей: механизма размножения и начинки.
6	Тема 1.5. Три вида возможных нарушений информационной системы	Понятие угрозы. Три вида возможных нарушений информационной системы. Под угрозой понимается потенциально возможные события, процесс или явление, которое может привести к уничтожению информации или утрате целостности, конфиденциальности или доступности информации.
7	Тема 1.6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные	Нормативно-справочные документы содержат нормы и нормативы, необходимые при решении задач организации и планирования труда в сфере материального производства и управления.
8	документы,Тема 1.7. Основные положения теории информационной безопасности	Изложены основные понятия теории информационной безопасности, методология построения систем защиты автоматизированных информационных систем (АС), раскрывается понятие формальных политик безопасности.
9	Тема 1.8. Назначение и задачи в сфере обеспечения информационной безопасности	Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
10	Тема 1.9. Модели безопасности и их применение	Модели безопасности и их применение. Метод формальной разработки системы опирается на модель безопасности (модель управления доступом, модель политики безопасности).
11	**Модуль 2. Защита информации**	Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
15	Тема 2.1. Использование защищенных компьютерных систем	Использование защищенных компьютерных систем. Межсетевой экран – инструмент реализации политики безопасности.
16	Тема 2.2. Методы криптографии	Что такое криптография. Криптография — наука, которая изучает методы обеспечения конфиденциальности, безопасности и аутентичности информации.
17	Тема 2.3. Основные технологии построения защищенных систем	Основные технологии построения защищённых. Экономические информационные системы. Общие принципы построения защищенных систем. Средства разработки и правила их реализации.
18	Тема 2.4 Место информационной безопасности экономических систем в национальной безопасности страны	Место информационной безопасности экономических систем в национальной безопасности страны. Internet и информационная безопасность несовместны по самой природе Internet.
19	Тема 2.5. Защита экономических систем	Защита экономической системы - это взаимосвязанный комплекс мер в политической, экономической, здравоохранительной, социальной, военной и правовой сферах.
20	Тема 2.6. Обмен конфиденциальной информацией	Конфиденциальная информация — это сведения, доступ к которым ограничен законом, а их разглашение наказуемо.
21	Тема 2.7. Структура банковских информационных систем в области защиты информации	Компания SearchInform – российский разработчик средств информационной безопасности и инструментов для защиты информации.
22	Тема 2.8. Важность защиты экономических систем	Защита экономической системы – это взаимоувязанный комплекс мероприятий в области политики, экономики, здравоохранения, социальной защиты, военной, правовой сферы.
23	Тема 2.9. Концепция информационной безопасности	Шаблоны типовых документов по информационной безопасности. Концепция обеспечения информационной безопасности предприятия.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1. Учебно-методическое обеспечение самостоятельной работы обучающихся

Таблица 5

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1.	Угрозы информационной безопасности	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
2.	Современные средства защиты информации	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
3.	Современные системы компьютерной безопасности	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
4.	Современные криптографические системы	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
5.	Криптоанализ, современное состояние	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
6.	Правовые основы защиты информации	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов

3.1 Учебно-методическое и информационное обеспечение программы дисциплины (модуля)

3.1.1. Основная и дополнительная литература

Основная литература

1. **Информационная безопасность:** учебник для вузов / под ред. Л. А. Ибрагимова. — М.: Юрайт, 2026. — 320 с.
2. **Основы информационной безопасности в ГМУ:** учебник для бакалавров / А. В. Смирнов, К. С. Петров. — СПб.: Питер, 2025. — 285 с.
3. **Правовое обеспечение информационной безопасности в РФ:** учебник / Е. М. Кузнецова. — М.: Инфра-М, 2025. — 310 с.
4. **Защита персональных данных в органах власти:** учебное пособие / под ред. Л. А. Дмитриева. — М.: КноРус, 2025. — 198 с.
5. **Безопасность государственных информационных систем (ГИС):** учебник / В. П. Сидоров. — М.: КноРус, 2025. — 276 с.
6. **Кибербезопасность и защита данных в цифровой экономике:** учебник / О. В. Морозова. — М.: Дашков и Ко, 2025. — 242 с.
7. **Информационное право и защита государственной тайны:** учебное пособие / под ред. Н. П. Тихонова. — М.: Инфра-М, 2025. — 215 с.
8. **Управление рисками информационной безопасности в ведомствах:** учебник / В. А. Соколов. — Новосибирск: НГТУ, 2024. — 220 с.
9. **Технические и криптографические методы защиты информации:** учебник / С. В. Николаев. — Екатеринбург: Изд-во УрФУ, 2024. — 254 с.
10. **Основы национальной безопасности и защита критической инфраструктуры:** учебное пособие / Т. А. Васильева. — СПб.: Лань, 2025. — 186 с.
11. **Противодействие киберугрозам и компьютерная преступность:** учебник / А. Д. Козлов. — М.: Дело РАНХиГС, 2024. — 230 с.
12. **Информационная безопасность электронного документооборота в ГМУ:** учебник / Р. С. Семенов. — М.: Юрайт, 2024. — 212 с.
13. **Аудит информационной безопасности в государственных учреждениях:** учебное пособие / И. В. Федоров. — М.: Юрайт, 2024. — 190 с.

14. **Организационное обеспечение информационной безопасности:** учебное пособие / М. А. Киселев. — Томск: Изд-во ТГУ, 2024. — 164 с.
15. **Информационная гигиена и цифровая грамотность служащих:** учебник / Е. П. Никитина. — М.: Магистр, 2023. — 210 с.
16. **Безопасность облачных технологий в публичном управлении:** учебное пособие / К. Д. Воробьев. — М.: РЭУ им. Г. В. Плеханова, 2025. — 175 с.
17. **Стандарты и регламенты информационной безопасности:** учебник / М. В. Чернов. — СПб.: Изд-во СПбГЭУ, 2024. — 218 с.
18. **Электронная подпись и биометрия: правовые и технические аспекты:** учебное пособие / А. А. Лебедев. — М.: Юрайт, 2024. — 156 с.
19. **Социальная инженерия и методы защиты от манипуляций в ИТ:** учебник / В. С. Горбунов. — М.: Инфра-М, 2024. — 240 с.
20. **Практикум по информационной безопасности: разбор инцидентов и кейсы:** учебное пособие / Д. М. Волков. — М.: Изд-во МГУ, 2023. — 145 с.

Дополнительная литература

21. **Доктрина информационной безопасности РФ: теория и практика реализации:** монография / И. В. Макаров, А. С. Смирнов. — СПб.: Питер, 2024. — 202 с.
22. **Методические рекомендации по обеспечению режима конфиденциальности в организации:** методические указания / под ред. И. И. Попова. — М.: Юрайт, 2023. — 94

3.1.2. Интернет-ресурсы

1. Электронно-библиотечная система IPRbooks (www.iprbookshop.ru)
2. Образовательная платформа «ЮРАЙТ» https://urait.ru/)
3. Электронно-библиотечная система «Лань» (https://e.lanbook.com/)
4. НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU (https://www.elibrary.ru/)
5. СПС «КонсультантПлюс» (http://www.consultant.ru/

3.2. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине необходима следующая материально-техническая база:

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 52. *683032, Камчатский край,* *г. Петропавловск-Камчатский,* ул. Пограничная д. 4, 65,7 кв. м., № 52	Учебная аудитория для проведения занятий лекционного типа, занятий лабораторного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 52. Основное оборудование: специализированная мебель учебная; проектор, экран; эксклюзивная документ камера; доска аудиторная, кушетка, манекен/симулятор, демонстрационные материалы, моноблок AQUARIUS с выходом в сеть Интернет и доступом к ЭБС – 20 шт.; компьютер

	QUARIUS с выходом в сеть Интернет и доступом к ЭБС – 1 шт.; МФУ – 1 шт.; интерактивная панель Lumien – 1 шт.; комплект учебного оборудования типовой «Криптографические системы» – 1 шт.; типовой комплект учебного оборудования «Сетевая безопасность» SECURITY – 1 шт.; доска подвижная маркерно/меловая – 1 шт. Используемое ПО: Microsoft Windows 10 (Лицензия ООО «Софистика» № 324 от 20.12.2018); Microsoft Office (Лицензия ООО «Софистика» № 324 от 20.12.2018); Антивирус Касперский (Лицензия № 0746B44B-A287-49F3-A1D7-77761279BB3E). GIMP; 7-ZIP; Anaconda; Google Chrome; Kdenlive; MySQL Workbench; Mobirise4; Firefox; NetEmul; ProjectLibre; Python; Ramus Educational; Scilab; TexLive; TexMaker; Acrobat Reader; Qt Designer; Corvid EVAL; DBeaver; Dev-C++; PostgreSQL; Visual Studio; Yandex; КОМПАС-3D LT