Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика и защита информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года 6 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Кандидат наук Ткаченко С. П.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Задачи изучения дисциплины:

- Освоить сновные подходы к защите данных от НСД;
- Изучить биометрические средства защиты информации и разграничения доступа.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Знать:

ПК-1.2/Зн1 Программные коды позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Уметь:

ПК-1.2/Ум1 Использовать программный код позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления

Владеть:

ПК-1.2/Нв1 Навыками создания программного кода позволяющего автоматизировать бизнес-процессы и решать задачи организационного управления

ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС

ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Знать:

ПК-2.2/Зн1 Какие необходимо принять меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Уметь:

ПК-2.2/Ум1 Сформулировать необходимые меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

Владеть:

ПК-2.2/Нв1 Инструментарием в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Программно-аппаратная защита информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-1 - Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы		
ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления	Безопасность Web-приложений, Безопасность мобильных приложений, Встроенные языки программирования, Методы и средства защиты информации, Организация вычислительных процессов, Основы алгоритмизации и программирования, Производственная практика: технологическая (проектно-технологическая) практика, Системы искусственного интеллекта, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Учебная практика: ознакомительная практика, Учебная практика: технологическая (проектно-технологическая) практика, Хранение, обработка и анализ данных	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Интеллектуальные информационные системы, Проектирование информационных систем, Проектный практикум, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Разработка профессиональных приложений, Современные цифровые технологии управления предприятием, Управление информационными проектами реализации комплексной безопасности
ПК-2 - Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС		
ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС	Безопасность Web-приложений, Безопасность мобильных приложений, Криптографическая защита информации, Методы и средства защиты информации, Организационная защита информации, Правовая защита информации, Производственная практика: технологическая (проектно-технологическая) практика, Теория информационной безопасности и методология защиты информации, Техническая защита информации, Учебная практика: технологическая (проектно-технологическая) практика	Безопасность Web-приложений, Безопасность мобильных приложений, Выполнение и защита выпускной квалификационной работы, Организационная защита информации, Производственная практика: преддипломная практика, Производственная практика: технологическая (проектно-технологическая) практика, Техническая защита информации

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лекционные занятия (часы)	Практические занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Седьмой семестр	108	3	4	2	2	0,15	85,85	Зачет
Всего	108	3	4	2	2	0,15	85,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС	**43**	**2**		**40,85**
Тема 1.1. Концепция построения программно–аппаратных средств обеспечения информационной безопасности.	43	2		40,85
Раздел 2. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС.	**47**		**2**	**45**
Тема 2.1. Методы ограничения доступа и управления доступом. Идентификация и аутентификация.	47		2	45

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	тестирование
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС	тестирование	Зачет
2	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС.	тестирование	Зачет

6. Оценочные материалы текущего контроля

1. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	К правовым методам, обеспечивающим информационную безопасность, относятся: - Разработка аппаратных средств обеспечения правовых данных - Разработка и установка во всех компьютерных правовых сетях журналов учета действий - Разработка и конкретизация правовых нормативных актов обеспечения безопасности		ПК-1
	Ответ:	Разработка и конкретизация правовых нормативных актов обеспечения безопасности	
2	Основными источниками угроз информационной безопасности являются все указанное в списке: - Хищение жестких дисков, подключение к сети, инсайдерство - Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы		ПК-1
	Ответ:	Перехват данных, хищение данных, изменение архитектуры системы	
3	Виды информационной безопасности: - Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная		ПК-2
	Ответ:	Персональная, корпоративная, государственная	
4	Цели информационной безопасности своевременное обнаружение, предупреждение - несанкционированного доступа - инсайдерства в организации - чрезвычайных ситуаций		ПК-2
	Ответ:	несанкционированного доступа	
5	Основные объекты информационной безопасности - Компьютерные сети, базы данных - Информационные системы, психологическое состояние пользователей - Бизнес-ориентированные, коммерческие системы		ПК-2
	Ответ:	Компьютерные сети, базы данных	

2. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с ИС. тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Основными рисками информационной безопасности являются - Искажение, уменьшение объема, перекодировка информации - Техническое вмешательство, выведение из строя оборудования сети - Потеря, искажение, утечка информации		,
	Ответ:	Потеря, искажение, утечка информации	

7. Оценочные материалы промежуточной аттестации

Зачет седьмой семестр

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Принципом политики информационной безопасности является принцип - Разделения доступа (обязанностей, привилегий) клиентам сети (системы) - Одноуровневой защиты сети, системы - Совместимых, однотипных программно-технических средств сети, системы		ПК-2
	Ответ:	Разделения доступа (обязанностей, привилегий) клиентам сети (системы)	
2	Когда получен спам по e-mail с приложенным файлом, следует - Прочитать приложение, если оно не содержит ничего ценного – удалить - Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама - Удалить письмо с приложением, не раскрывая (не читая) его		ПК-1
	Ответ:	Удалить письмо с приложением, не раскрывая (не читая) его	
3	Принцип Кирхгофа - Секретность ключа определена секретностью открытого сообщения - Секретность информации определена скоростью передачи данных - Секретность закрытого сообщения определяется секретностью ключа		ПК-1
	Ответ:	Секретность закрытого сообщения определяется секретностью ключа	
4	ЭЦП – это - Электронно-цифровой преобразователь - Электронно-цифровая подпись - Электронно-цифровой процессор		ПК-2
	Ответ:	Электронно-цифровая подпись	
5	Утечкой информации в системе называется ситуация, характеризуемая - Потерей данных в системе - Изменением формы информации - Изменением содержания информации		ПК-1
	Ответ:	Потерей данных в системе	

7.1. Уровни овладения

Компетенция: ПК-1 Способен к разработке прототипов ИС и к созданию программного кода ИС в рамках выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы.

Индикатор достижения компетенции: ПК-1.2 Создает программный код ИС, позволяющий автоматизировать бизнес-процессы и решать задачи организационного управления.

Уровень	Характеристика
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять программный код ИС для решения задач организационного управления в различных ситуациях для решения поставленных задач.
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять программный код ИС для решения задач организационного управления в различных ситуациях для решения поставленных задач.
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять программный код ИС для решения задач организационного управления в стандартных ситуациях.
Ниже порогового	Компетенция не освоена

Компетенция: ПК-2 Способен к тестированию ИС и принятию мер при обнаружении инцидентов информационной безопасности, связанных с работой ИС, в рамках выполнения работ по созданию (модификации) и сопровождению ИС.

Индикатор достижения компетенции: ПК-2.2 Принимает меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС.

Уровень	Характеристика
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС в различных ситуациях для решения поставленных задач.
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС в различных ситуациях для решения поставленных задач.
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять меры в случае обнаружения инцидентов ИБ, связанных с работой ИС, в рамках выполнения работ по созданию и сопровождению ИС для решения поставленных задач в стандартных ситуациях.
Ниже порогового	Компетенция не освоена

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. - 2-е изд. - Москва: Юрайт, 2026. - 107 с - 978-5-534-16388-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588741 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Внуков, А. А. Защита информации в банковских системах: учебник для вузов / А. А. Внуков. - 2-е изд. - Москва: Юрайт, 2026. - 246 с - 978-5-534-01679-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/584051 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. http://www.gov.ru/ - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия»

Ресурсы «Интернет»

1. https://digital.gov.ru - Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)

2. https://lms2.sseu.ru - БРСО

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
1. 7-Zip;
2. «Альт Образование» и/или «Альт Рабочая станция»;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
1. Справочно-правовая система "Гарант-Максимум";

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения