Министерство просвещения Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Уральский государственный педагогический университет»

Факультет естествознания, математики и информатики
Кафедра информационных технологий и физико-математического образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Программа подготовки специалистов среднего звена среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением

Автор(ы): канд. пед. наук, доцент, доцент кафедры ИТФМ Е. С. Васева

Одобрена на заседании кафедры информационных технологий и физико-математического образования. Протокол от 27 апреля 2026 г. № 7.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией факультета естествознания, математики и информатики. Протокол от 27 апреля 2026 г. № 7.

Нижний Тагил
2026

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Программа учебной дисциплины ОП.05. «Основы информационной безопасности» составлена в соответствии с Федеральным государственным образовательным стандартом (далее ФГОС) по специальности среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением, утвержденным приказом Министерства просвещения РФ от 24 февраля 2025 года № 138.

1.1. Область применения программы

Программа учебной дисциплины ОП.05. «Основы информационной безопасности» предназначена для ведения занятий со студентами очной формы обучения, осваивающими программу подготовки специалистов среднего звена среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2. Место дисциплины в структуре ППССЗ

Дисциплина ОП.05. «Основы информационной безопасности» входит в общепрофессиональный цикл профессиональной подготовки программы подготовки специалистов среднего звена среднего профессионального образования по профессии 09.02.11 Разработка и управление программным обеспечением. Учебным планом предусмотрено изучение данной дисциплины на втором курсе (4 семестр).

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате изучения дисциплины ОП.05. «Основы информационной безопасности» обучающийся должен:

Иметь практический опыт:	Разработки политик ИБ и регламентов обработки персональных данных. Работы с инструментами аудита ИБ. Резервного копирования и восстановления данных после имитации сбоя или атаки.
Уметь:	классифицировать защищаемую информацию по видам тайны и степеням секретности классифицировать основные угрозы безопасности информации;
Знать:	сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины

максимальной учебной нагрузки – 32 часа, в том числе:

обязательной аудиторной учебной нагрузки – 32 часа (в том числе лекции 12 часов, лабораторные занятия 20 часов).

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Применение данной программы направлено на формирование элементов основных видов профессиональной деятельности в части освоения соответствующих общих (ОК) и профессиональных компетенций (ПК):

Код	Наименование результата обучения
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

Код	Наименование видов деятельности и профессиональных компетенций
ПК 1.1.	Проектировать базы данных
ПК 1.4.	Администрировать базы данных
ПК 1.5.	Защищать информацию в базе данных с использованием технологии защиты информации
ПК 3.1.	Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика
ПК 3.2.	Разрабатывать веб-приложения в соответствии с техническим заданием
ПК 3.3.	Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием
ПК 3.5.	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности
ПК 3.7.	Реализовывать мероприятия по продвижению приложения

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Максимальная учебная нагрузка	**32**
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
теоретическое обучение	12
лабораторные занятия	20
Промежуточная аттестация	
проводится в форме зачета с оценкой в 4 семестре	

3.2. Тематический план и содержание учебной дисциплины

ОП.05. «Основы информационной безопасности»

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся.	Объем в часах	Осваиваемые элементы компетенций
Раздел 1. Теоретические основы информационной безопасности		**20**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание**	**4**	ОК 01.; ОК 02.; ОК 09.
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.		
	В том числе, практических занятий и лабораторных работ	2	
	1. Оценка угроз и рисков информационной безопасности: анализ кейсов киберпреступлений	2	
Тема 1.2. Основы защиты информации	**Содержание**	**6**	ОК 01.; ОК 02.; ОК 09.; ПК 1.1.; ПК 1.4.; ПК 1.5.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.5.; ПК 3.7.
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.		
	В том числе, практических занятий и лабораторных работ	4	
	2. Определение объектов защиты на типовом объекте информатизации.	2	
	3. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
Тема 1.3. Угрозы безопасности защищаемой информации	**Содержание**	**10**	ОК 01.; ОК 02.; ОК 09.; ПК 1.1.; ПК 1.4.; ПК 1.5.; ПК 3.1.;
	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации		

	В том числе, практических занятий и лабораторных работ	6	ПК 3.2.; ПК 3.3.; ПК 3.5.; ПК 3.7.
	4. Определение угроз объекта информатизации и их классификация	2	
	5. Составление частной модели угроз. Установление исходного уровня защищенности	2	
	6. Составление частной модели угроз. Составление актуального списка угроз	2	
Раздел 2. Методология защиты информации		**16**	
Тема 2.1. Методологические подходы к защите информации	**Содержание**	**4**	ОК 01.; ОК 02.; ОК 09.
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.		
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание**	**8**	ПК 1.1.; ПК 1.4.; ПК 1.5.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.5.; ПК 3.7.
	Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации		
	В том числе, практических занятий и лабораторных работ	6	
	7. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2	
	8. Поиск и анализ требований ФЗ 152-ФЗ к защите персональных данных в информационных системах	2	
	9. Сравнительный анализ российского и международного регулирования в области информационной безопасности	2	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание**	**4**	ПК 1.1.; ПК 1.4.; ПК 1.5.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.5.; ПК 3.7.
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		
	В том числе, практических занятий и лабораторных работ	2	
	10. Выбор мер защиты информации для автоматизированного рабочего места	2	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Требования к материально-техническому обеспечению:

Реализация учебной программы осуществляется в кабинете информатики.

Учебная аудитория для проведения занятий лекционного типа, семинарского (практического), лабораторного типа, курсового проектирования (выполнения курсовых работ), проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации:

комплект учебной мебели для обучающихся (12 посадочных мест);

комплект мебели для преподавателя (1 рабочее место);

технические средства обучения: переносной мультимедиа комплекс (ноутбук, проектор), экран, маркерная доска, лазерный принтер (МФУ) А4 – 1 шт.; компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации (компьютер – 12 шт.);

вспомогательные средства обучения: наборы учебно-наглядных пособий, плакаты, макеты, фотографии, видеоматериалы;

комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

операционные системы семейства Windows NT корпорации Microsoft;

Kaspersky Endpoint Security для Windows;

FoxitReader программа для чтения PDF файлов;

Залы: библиотека, читальный зал с выходом в сеть Интернет.

4.2. Информационное обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458 (дата обращения: 26.04.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374 (дата обращения: 26.04.2026).

3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457 (дата обращения: 26.04.2026).

Дополнительная литература

1. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Профессиональное образование). — ISBN 978-5-

534-20645-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590435 (дата обращения: 26.04.2026).

2. Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Профессиональное образование). — ISBN 978-5-534-20505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590434 (дата обращения: 26.04.2026).

3. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372 (дата обращения: 26.04.2026).

Электронные ресурсы

Портал «Российская электронная школа» https://resh.edu.ru/
Цифровая библиотека IPRsmart https://www.iprbookshop.ru/
Электронно-библиотечная система АЙбукс https://ibooks.ru/
Электронно-библиотечная система ЛАНЬ https://e.lanbook.com/
Образовательная платформа ЮРАЙТ https://urait.ru/

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Нижнетагильский государственный социально-педагогический институт (филиал) ФГАОУ ВО «УрГПУ», реализующий подготовку по данной учебной дисциплине, обеспечивает организацию и проведение промежуточной аттестации и текущего контроля индивидуальных образовательных достижений – демонстрируемых студентами знаний, умений и навыков.

Текущий контроль проводится преподавателем в процессе проведения практических и лабораторных занятий, а также выполнения студентами индивидуальных творческих заданий, исследований, решения проблемных задач.

Освоение учебной дисциплины завершается промежуточной аттестацией, которую проводит педагог.

Для промежуточной аттестации и текущего контроля создан фонд контрольно-оценочных средств (ФОС).

ФОС включает в себя педагогические контрольно-измерительные материалы, предназначенные для определения соответствия (или несоответствия) индивидуальных образовательных достижений основным показателям результатов подготовки (таблицы), а также памятки, алгоритмы для выполнения студентами различных видов работ.

Результаты (освоенные умения, знания)	**Основные показатели результатов**	**Формы и методы контроля**
Знает: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченногодоступа в процессе ее создания, обработки, передачи; современные средстваи способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности.	Демонстрирует знания основ информационной безопасности	Экспертное наблюдение выполнения практических работ
Умеет: Классифицировать защищаемую информацию повидам тайны и степенямсекретности; классифицировать основные угрозы безопасностиинформации	Проявляет способность классифицировать защищаемую информацию повидам тайны и степеням секретности; классифицировать основные угрозы безопасности информации	Экспертное наблюдение выполнения практических работ

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций,

но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общекультурные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	Выбирает способы защиты информации с учётом контекста: тип системы, требования заказчика, нормативные ограничения	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Использует инструменты для аудита ИБ, выполняет поиск и анализ нормативных актов (КонсультантПлюс, pravo.gov.ru)	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Способен работать с международными стандартами	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ПК 1.1. Проектировать базы данных ПК 1.4. Администрировать базы данных ПК 1.5.Защищать информацию в базе данных с использованием технологии защиты информации	Проектирует и администрирует БД с учётом требований ИБ: шифрование, разграничение доступа, аудит операций	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ПК 3.1. Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика ПК 3.2. Разрабатывать веб-приложения в соответствии с техническим заданием	Разрабатывает ТЗ на веб-приложения с учётом требований безопасности	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ПК 3.3. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием	Выполняет техническое сопровождение веб-приложений: мониторинг безопасности, обновление мер защиты, восстановление после инцидентов	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач
ПК 3.5. Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности	Выполняет аудит безопасности веб-приложений по регламенту: сканирование уязвимостей, тестирование на проникновение, составление отчётов	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач

ПК 3.7. Реализовывать мероприятия по продвижению приложения	Реализовывает мероприятия по продвижению веб-приложений с учётом требований ИБ: защита данных пользователей	Наблюдение за организацией деятельности на занятиях, опрос, собеседование, тестирование, оценка решения ситуационных задач

Типовые задания для проведения процедуры оценивания результатов освоения дисциплины в ходе промежуточной аттестации

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

1. Какой способ защиты информации следует выбрать для веб-приложения, обрабатывающего персональные данные?

а) только антивирусное ПО;

б) шифрование данных и разграничение доступа;

в) резервное копирование раз в месяц;

г) отключение интернет-соединения.

2. В какой ситуации наиболее целесообразно применение DLP-системы?

а) при необходимости ускорения работы сети;

б) для предотвращения утечек конфиденциальной информации;

в) для увеличения объёма хранилища данных;

г) для настройки Wi-Fi сети.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

1. Какой инструмент лучше всего подходит для сканирования сети на уязвимости?

а) Microsoft Word;

б) Nmap;

в) Paint;

г) Калькулятор.

2. Какой инструмент используют для анализа сетевого трафика?

a) Excel;

b) Wireshark;

c) PowerPoint;

d) Блокнот.

Правильный ответ: b)

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках

1. Что означает термин «CIA triad» в ИБ?

а) Central Intelligence Agency;

б) Confidentiality, Integrity, Availability;

в) Computer Information Access;

г) Cyber Incident Analysis.

2. Как переводится «Data Breach»?

а) утечка данных;

б) резервное копирование;

в) шифрование;

г) аутентификация.

ПК 1.1. Проектировать базы данных

1. Какой тип данных лучше использовать для хранения паролей?

а) VARCHAR без шифрования;

б) HASHED (хешированные);

в) INTEGER;
г) TEXT в открытом виде.

2. Какой механизм предотвращает SQL-инъекции при проектировании БД?
а) использование динамического SQL;
b) параметризованные запросы;
c) хранение паролей в открытом виде;
d) отключение логирования.

ПК 1.4. Администрировать базы данных

1. Какая команда предоставляет права доступа пользователю в SQL?
а) DROP USER;
б) GRANT SELECT;
в) DELETE DATABASE;
г) CREATE TABLE.

2. Что такое аудит БД?
а) удаление данных;
б) мониторинг и регистрация действий пользователей;
в) форматирование диска;
г) обновление ОС.

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации

1. Какой метод обеспечивает шифрование данных в БД?
а) TDE (Transparent Data Encryption);
б) увеличение объёма ОЗУ;
в) смена имени сервера;
г) отключение сети.

2. Какой стандарт регламентирует защиту данных в платёжных системах?
a) PCI DSS;
b) ISO 9001;
c) ГОСТ Р 34.10;
d) IEEE 802.11.

ПК 3.1. Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика

Какой раздел ТЗ должен включать требования к ИБ?
а) дизайн интерфейса;
б) функциональные требования и безопасность;
в) список шрифтов;
г) цветовая схема.

2. Какой стандарт описывает требования к безопасной разработке?
a) ISO/IEC 27034;
b) ГОСТ Р ИСО 9001;
c) IEEE 754;
d) RFC 2616.

ПК 3.2. Разрабатывать веб-приложения в соответствии с техническим заданием

1. Какой метод предотвращает XSS-атаки в веб-приложении?

а) использование Content Security Policy (CSP) с запретом inline-скриптов;
б) экранирование пользовательского ввода на стороне клиента;
в) отключение JavaScript во всех браузерах;
г) хранение данных в localStorage без дополнительных проверок.

2. Какой протокол следует использовать для защищённой передачи данных в веб-приложении?
a) HTTP с базовой аутентификацией;
b) FTP с SSL-шифрованием;
c) HTTPS с поддержкой TLS 1.3;
d) WebSocket без шифрования.

ПК 3.3. Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием

1. Что нужно сделать в первую очередь при обнаружении утечки данных?
а) удалить логи для экономии места;
б) изолировать затронутые системы и ограничить доступ;
в) уведомить всех пользователей по электронной почте;
г) перезагрузить сервер для сброса состояния.

2. Как часто следует обновлять ПО веб-приложения?
а) только при появлении новых функций;
б) при выпуске критических обновлений безопасности и патчей уязвимостей;
в) раз в год, во время планового техобслуживания;
г) только после уведомления хостинг-провайдера.

ПК 3.5. Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

1. Какой инструмент используют для автоматизированного сканирования уязвимостей веб-приложений?
а) Microsoft Word с макросами;
б) OWASP ZAP в режиме активного сканирования;
в) PowerPoint для визуализации архитектуры;
г) Excel для составления таблиц рисков.

2. Что включает аудит безопасности веб-приложения?
а) проверку цветовой схемы интерфейса на соответствие брендбуку;
б) тестирование на проникновение, анализ кода и конфигураций;
в) подсчёт количества страниц и ссылок;

3. Опишите пошаговый процесс аудита безопасности веб-приложения с использованием OWASP ZAP. Укажите, какие типы уязвимостей проверяются в первую очередь (например, OWASP Top 10), и как интерпретировать результаты сканирования.

ПК 3.7. Реализовывать мероприятия по продвижению приложения

1. Какое требование ИБ необходимо учитывать при продвижении приложения с обработкой ПДн?
а) сбор данных без согласия пользователей для повышения конверсии;
б) соответствие ФЗ 152-ФЗ и GDPR, включая механизмы отзыва согласия;
в) публикация всех данных в открытом доступе для прозрачности;
г) отключение шифрования для ускорения загрузки страниц.

2. Какой элемент продвижения требует особого внимания с точки зрения ИБ?
а) цвет логотипа на рекламных баннерах;
б) формы сбора контактных данных с валидацией и шифрованием;
в) шрифт заголовков в email-рассылках;
г) расположение баннеров на партнёрских сайтах.