Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Проректор
_____ / А.А. Кирсанкин/
«__»_____ 2026 г.

Рабочая программа учебной дисциплины

БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

образовательной программы высшего образования –
программы специалитета

10.05.03 Информационная безопасность автоматизированных систем
Специализация №5 "Безопасность открытых информационных систем"

Форма обучения: очная

Курган 2026

Рабочая программа дисциплины «Безопасная разработка программного обеспечения» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения «30» июня 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «02» сентября 2026, протокол № 1.

Рабочую программу составил:
канд. биол. наук, доцент А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		11
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	32	32
Самостоятельная работа, всего часов в том числе:	**80**	**80**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	62	62
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Безопасная разработка программного обеспечения» относится к части, формируемой участниками образовательных отношений дисциплинам Блока Б1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин: Программно-аппаратные средства защиты информации; Безопасность информационных систем; Аппаратные средства вычислительной техники.

Результаты обучения по дисциплине необходимы для изучения дисциплин «Анализ уязвимостей и тестирование на проникновение информационных систем», для прохождения преддипломной практики, а также для выполнения выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Безопасная разработка программного обеспечения» является алгоритмизации и составления безопасного программного обеспечения на алгоритмическом языке высокого уровня с использованием процедурного и событийного программирования, а также современных технологий создания программных средств.

Задачи дисциплины:

- овладение методами безопасного программирования и методами разработки эффективных алгоритмов решения прикладных задач;
- сформировать представление об общих принципах и методах построения безопасных программ с текстовым и графическим интерфейсом.

Компетенции, формируемые в результате освоения дисциплины:

- Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-5);
- Способен оценивать эффективность систем защиты информации, функционирующих в открытых информационных системах (ПК-8).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины обеспечения», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Безопасная разработка программного обеспечения», индикаторы достижения компетенций ПК-5, ПК-8, перечень оценочных средств представлены в таблице.

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1 ПК-5	– Знать: основные проектные решения по обеспечению безопасности	З (ИД-1 ПК-5)	Знает: основные проектные решения по обеспечению	Вопросы теста

		автоматизированных систем		безопасности автоматизированных систем и их анализ	
2.	ИД-2 ПК-5	– Уметь: разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	У (ИД-2 ПК-5)	Умеет: разрабатывать проектные решения по обеспечению безопасности автоматизированных систем	Комплекс имитационных задач
3.	ИД-3 ПК-5	– Владеть: методами проектных решений по обеспечению безопасности автоматизированных систем	В (ИД-3 ПК-5)	Владеет: методами проектных решений по обеспечению безопасности автоматизированных систем	Комплекс имитационных задач
4.	ИД-1 ПК-8	– Знать: эффективные способы защиты информации в системах	З (ИД-1 ПК-8)	Знает: основные уязвимости и эффективные способы защиты информации в системах	Вопросы теста
5.	ИД-2 ПК-8	– Уметь: оценивать эффективность систем защиты	У (ИД-2 ПК-8)	Умеет: оценивать эффективность систем защиты и обеспечивать тестирование систем на проникновение	Комплекс имитационных задач
6.	ИД-3 ПК-8	– Владеть: навыками оценки эффективности систем защиты информации в открытых системах	В (ИД-3 ПК-8)	Владеет: навыки анализа программных реализаций на предмет оценки эффективности систем защиты информации	Комплекс имитационных задач

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Очная	
			Лекции	Лабор.
Рубеж 1	Тема 1	*Введение в безопасную разработку и нормативная база*	4	2
	Тема 2	*Моделирование угроз и проектирование архитектуры безопасности*	4	4
	Тема 3	*Безопасная разработка исходного кода*	4	4
	Тема 4	*Управление сторонними компонентами и цепочкой поставок*	4	4
		1-ый рубежный контроль Тестирование	-	1
Рубеж 2	Тема 5	*Безопасная сборка, хранение артефактов и управление секретами*	4	4
	Тема 6	*Тестирование на проникновение и динамический анализ*	4	4
	Тема 7	*Безопасный релиз, эксплуатация и реагирование на инциденты*	4	4
	Тема 8	*Внедрение SDL (Secure Development Lifecycle)*	4	4
		2-ый рубежный контроль Тестирование	-	1
		Всего:	**32**	**32**

4.2. Содержание лекционных занятий

Тема 1. Введение в безопасную разработку и нормативная база.

История появления стандартов безопасной разработки. Разница между функциональным тестированием и поиском уязвимостей. Обзор ГОСТ Р 56939-2016: область применения, основные термины (уязвимость, недекларированная возможность, жизненный цикл ПО).ьМесто ГОСТ Р 56939 в экосистеме российских стандартов (связь с ГОСТ Р 57580.1 для финансовых организаций, требования ФСТЭК России). Международные аналоги: OWASP SAMM, BSIMM, NIST Secure Software Development Framework (SSDF). Экономическое обоснование: стоимость исправления уязвимости на разных этапах SDLC (правило «десятикратных затрат»).

Тема 2. Моделирование угроз и проектирование архитектуры безопасности.

Процесс создания модели угроз по методологии ФСТЭК России. Идентификация активов, нарушителей и уязвимостей. Методики STRIDE (Microsoft) и PASTA для классификации угроз (Spoofing, Tampering,

Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Проектирование безопасного приложения: принцип наименьших привилегий, эшелонированная оборона, безопасные фреймворки. Формирование требований к безопасности: функциональные (что система должна делать) и нефункциональные (как она должна это делать безопасно).

Тема 3. Безопасная разработка исходного кода.

Классификация дефектов кода, приводящих к уязвимостям (OWASP Top 10, CWE/SANS Top 25). Обзор уязвимостей: SQL-инъекции, межсайтовый скриптинг (XSS), небезопасная десериализация, некорректное управление доступом (IDOR). Принципы безопасного кодирования: валидация и санитизация входных данных, параметризованные запросы, использование подготовленных выражений (prepared statements), безопасная работа с криптографией. Обзор инструментов статического анализа (SAST) и их интеграция в IDE.

Тема 4. Управление сторонними компонентами и цепочкой поставок.

Риски использования Open Source: уязвимости в библиотеках (пример Log4Shell), лицензионная чистота. Составление SBOM (Software Bill of Materials) — перечня всех сторонних компонентов. Процесс управления цепочкой поставок (SSCS). Проверка репутации репозиториев. Инструменты анализа состава ПО (SCA — Software Composition Analysis).

Тема 5. Безопасная сборка, хранение артефактов и управление секретами.

Защита сборочного конвейера (CI/CD). Подписание кода и артефактов (Code Signing). Безопасное хранение артефактов в репозиториях (Nexus, Artifactory). Проблема секретов в коде: API-ключи, пароли, сертификаты. Использование менеджеров секретов (HashiCorp Vault) и переменных окружения. Контейнерная безопасность: сканирование образов Docker на наличие уязвимостей ОС и ПО.

Тема 6. Тестирование на проникновение и динамический анализ.

Разница между SAST, DAST (Dynamic Application Security Testing) и IAST. Методология тестирования на проникновение веб-приложений (OWASP Testing Guide). Инструменты автоматизированного сканирования (OWASP ZAP, Burp Suite). Фаззинг-тестирование (Fuzzing) для поиска ошибок при обработке некорректных данных.

Тема 7. Безопасный релиз, эксплуатация и реагирование на инциденты.

Процесс управления уязвимостями (Vulnerability Management): от получения CVE до установки патча. Настройка безопасного конфигурирования среды (Hardening): отключение лишних портов и сервисов, настройка TLS, заголовков безопасности (HSTS, CSP). Логирование и мониторинг безопасности. Стандарты ведения логов. План реагирования на инциденты ИБ в разработке (PSIRT — Product Security Incident Response Team).

Тема 8. Внедрение SDL (Secure Development Lifecycle).

Объединение процессов разработки в единый регламент для ИТ-компании. Ролевая модель (владелец продукта, архитектор, разработчик, AppSec-инженер). Метрики эффективности процесса безопасной разработки (MTTD — Mean Time To Detect, MTTR — Mean Time To Remediate).

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ.	Норматив времени, час.
			очная
1	Тема 1	Лабораторная работа № 1. **Аудит документации.** Задача: провести первичный анализ ТЗ на соответствие требованиям ГОСТ Р 56939, выявить отсутствующие разделы (требования к аутентификации, шифрованию, обработке ошибок) и составить протокол замечаний.	2
2	Тема 2	Лабораторная работа № 2. **Моделирование угроз.** Система внутреннего кадрового учета: построить диаграммы потоков данных (DFD), выделить границы доверия, идентифицировать угрозы по методу STRIDE и оценить их по классической матрице (вероятность * ущерб). Результат оформить в виде реестра угроз.	4
3	Тема 3	Лабораторная работа № 3. **SAST и рефакторинг.** Задача: в веб-приложении с внесенными уязвимостями запустить анализатор (например, SonarQube, GitHub CodeQL или отечественный Solar appScreener), проанализировать отчет, исправить уязвимости в коде и добиться нулевого уровня критических дефектов.	4
4	Тема 4	Лабораторная работа № 4. **Анализ зависимостей.** С помощью SCA-инструмента (OWASP Dependency-Check, Snyk или российских аналогов) сканировать проект, в котором находится известная уязвимость библиотеки, найти уязвимый компонент, изучить CVE и обновить библиотеку до безопасной версии с сохранением работоспособности приложения.	4
	1-ый рубеж	***Тестирование***	**1**
5	Тема 5	Лабораторная работа № 5. **Hardening CI/CD.** Настроить пайплайн (например, в GitLab CI или Jenkins). Задачи: вынести жестко закодированные пароли из скриптов в защищенное хранилище, настроить шаг автоматического сканирования Docker-образа (Trivy) и запретить деплой в тестовую среду, если сканер нашел уязвимости уровня High.	4

6	Тема 6	Лабораторная работа № 6. **DAST-аудит.** Развернуть тестовый стенд (например, DVWA — Damn Vulnerable Web Application). С помощью OWASP ZAP или Burp Suite провести автоматизированный и ручной поиск уязвимостей (XSS, SQLi), их эксплуатацию в изолированной среде и зафиксировать успешность атаки (PoC — Proof of Concept).	4
7	Тема 7	Лабораторная работа № 7. **Настройка WAF и мониторинг.** Развернуть базовое веб-приложение и провести его защиту с помощью Web Application Firewall (например, ModSecurity для Apache/Nginx). Имитировать атаку (множественные попытки SQLi) и настроить правило, которое блокирует атакующего и отправляет оповещение в консоль мониторинга.	4
8	Тема 8	Лабораторная работа № 8. **Подготовка безопасного проекта к внедрению в работу.** Разработчикам выдается базовый, небезопасный проект. Задача — за ограниченное время (эквивалент 2 недель спринта) провести его через все этапы ГОСТ Р 56939: доработать ТЗ, исправить код по отчету SAST, обновить зависимости (SCA), пройти DAST-тестирование и подготовить регламент безопасной эксплуатации. Служба ИБ выступает в роли аудитора, выдавая замечания на каждом этапе.	4
	2-ой рубеж	***Тестирование***	**1**
		Итого	**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, подготовку к рубежным контролям и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы
Очная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**44**
Введение в безопасную разработку и нормативная база	5
Моделирование угроз и проектирование архитектуры безопасности	5
Безопасная разработка исходного кода	5
Управление сторонними компонентами и цепочкой поставок	5
Безопасная сборка, хранение артефактов и управление секретами	6
Тестирование на проникновение и динамический анализ	6
Безопасный релиз, эксплуатация и реагирование на инциденты	6
Внедрение SDL (Secure Development Lifecycle)	6
Подготовка к лабораторным работам (по 1 часа на каждое занятие)	16
Подготовка к рубежным контролям (по 1часа на каждый рубежный контроль)	2
Подготовка к зачету	18
Всего:	**80**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (очная форма).
2. Отчеты обучающихся по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2 (очная форма).
4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения обучающихся на первом учебном занятии)</td><td colspan="6">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение лабораторной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет</td></tr>
<tr><td>Балльная оценка:</td><td>0,5_б х 16= 8_б</td><td>5_б х 8 =40_б</td><td>11</td><td>11</td><td>30</td></tr>
<tr><td>2</td><td colspan="2">Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="5">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td colspan="2">Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="5">Для допуска к промежуточной аттестации по дисциплине за семестр, обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается.
Для получения зачета без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность.
Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается.
За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30.
Основанием для получения дополнительных баллов являются:
- выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем;
- участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 11 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 1 академический час.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающемуся отводится 1 астрономический час. Каждый вопрос оценивается до 15 баллов.

Результаты успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежного контроля и зачета

1-ый рубежный контроль

Вопрос 1. В рамках методологии ФСТЭК России при создании модели угроз эксперт идентифицировал базу данных с персональными данными, внешнего хакера и отсутствие патчей в веб-сервере. Что из перечисленного относится к уязвимостям?

а) база данных с персональными данными;

б) внешний хакер;

в) отсутствие патчей в веб-сервере;

г) внешний канал связи.

Вопрос 2. При классификации угроз по методологии STRIDE для веб-приложения обнаружена возможность подмены сессии пользователя путем кражи session_id. К какой категории STRIDE относится данная угроза?

а) spoofing (подмена личности);

б) tampering (целостность);

в) repudiation (отказ от авторства);

г) elevation of Privilege (повышение привилегий).

Вопрос 3. В проекте используется библиотека log4j версии 2.14.1. внезапно становится известно об уязвимости Log4Shell (CVE-2021-44228), позволяющей выполнить произвольный код через JNDI. Какой тип инструмента и какой первоочередной шаг необходимы для оценки масштаба проблемы во всем портфеле ПО компании?

а) SAST (провести статический анализ исходного кода на наличие импортов log4j);

б) SCA (Software Composition Analysis) (составить или актуализировать SBOM (Software Bill of Materials) для всех приложений и проверить его на наличие уязвимой версии);

в) DAST (просканировать запущенные веб-приложения на наличие полей ввода);

г) IAST (внедрить агент в JVM для поиска аномалий во время выполнения).

2-ой рубежный контроль

Вопрос 1. При хранении артефактов в репозитории Nexus или Artifactory необходимо обеспечить защиту от подмены уже опубликованной версии библиотеки (атака Supply Chain). Какая комбинация настроек решает эту проблему?

а) Включение принудительного TLS для доступа к репозиторию и настройка ротации паролей администраторов.

б) Включение политики блокировки перезаписи (Overwrite / Delete) для релизных репозиториев и внедрение обязательной проверки цифровой подписи артефактов (Code Signing) на стороне клиента перед использованием.

в) Хранение артефактов в публичном облаке и ограничение доступа по IP-адресу.

г) Ежедневное сканирование репозитория антивирусом и сжатие артефактов для экономии места.

Вопрос 2. При проведении тестирования веб-приложения согласно методологии OWASP Testing Guide, на каком этапе и с какой целью применяется фаззинг-тестирование (Fuzzing)?

а) На этапе сбора информации (Information Gathering) для поиска скрытых файлов и директорий по словарю.

б) На этапе валидации входных данных (Input Validation Testing) для передачи приложению заведомо некорректных, случайных или

переполняющих буфер данных с целью вызвать сбой, утечку памяти или обход авторизации.

в) На этапе проверки криптографии для подбора ключей шифрования методом грубой силы.

г) На этапе тестирования бизнес-логики для поиска скрытых скидок в корзине интернет-магазина.

Вопрос 3. При настройке безопасного конфигурирования веб-сервера (Hardening) заголовок Content-Security-Policy (CSP) предназначен для:

а) принудительного использования протокола HTTPS вместо HTTP (перенаправление);

б) защиты от межсайтового скриптинга (XSS) путем строгого указания доверенных источников, из которых браузеру разрешено загружать скрипты, стили и другой контент;

в) сокрытия версии веб-сервера (Server-Timing) от злоумышленника;

г) ограничения размера HTTP-заголовков для защиты от атак типа Buffer Overflow.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Какова область применения национального стандарта ГОСТ Р 56939-2016?
2. Дайте определения терминам «уязвимость» и «недекларированная возможность» согласно ГОСТ Р 56939-2016.
3. Как определяет «жизненный цикл программного обеспечения» стандарт ГОСТ Р 56939-2016?
4. Какое место занимает ГОСТ Р 56939-2016 в экосистеме российских стандартов и как он связан с ГОСТ Р 57580.1?
5. Какие требования регуляторов (ФСТЭК России) определяют необходимость применения практик безопасной разработки?
6. Назовите три ключевых международных фреймворка безопасной разработки и кратко опишите их назначение (OWASP SAMM, BSIMM, NIST SSDF).
7. В чем разница между подходами OWASP SAMM и BSIMM к оценке зрелости процессов разработки?
8. Сформулируйте экономическое обоснование внедрения SDLC. Как работает правило «десятикратных затрат» на разных этапах жизненного цикла?
9. Опишите основные этапы процесса создания модели угроз по методологии ФСТЭК России.
10. Что такое идентификатор актива, типы нарушителей и способы их идентификации при моделировании угроз?
11. В чем заключается основная идея методологии PASTA и чем она принципиально отличается от STRIDE.
12. Что такое эшелонированная оборона (Defense in Depth) и как она реализуется на уровне приложения?

13. В чем разница между функциональными и нефункциональными требованиями к безопасности? Приведите примеры для каждого типа.
14. Как результаты моделирования угроз трансформируются в конкретные задачи для команды разработки (user stories)?
15. Назовите три наиболее критичные уязвимости из списка OWASP Top 10 (2021) и кратко опишите механизм их работы.
16. Что такое CWE и как он связан с OWASP Top 10? Приведите примеры из CWE/SANS Top 25.
17. В чем опасность небезопасной десериализации данных и как ее предотвратить?
18. Что такое уязвимость IDOR (Insecure Direct Object Reference) и как она связана с некорректным управлением доступом?
19. Назовите три популярных инструмента статического анализа кода и опишите их интеграцию в IDE разработчика.
20. Почему внедрение SAST на этапе написания кода (shift-left) эффективнее, чем на этапе тестирования готового продукта?
21. Почему проверка лицензионной чистоты сторонних компонентов важна для коммерческого продукта?
22. По каким критериям оценивается репутация репозитория (например, на GitHub) перед подключением зависимости?
23. Какие основные меры защиты применяются для изоляции и защиты сборочного конвейера (CI/CD)?
24. Как работают менеджеры секретов (на примере HashiCorp Vault) и чем они лучше переменных окружения?
25. Опишите процесс безопасного деплоя секретов в контейнеризованное приложение.
26. Что такое сканирование Docker-образов и какие типы уязвимостей (ОС, ПО) оно позволяет выявить?
27. Что такое «минимальный базовый образ» и почему его использование повышает безопасность контейнера?
28. В чем принципиальная разница между SAST, DAST и IAST? На каком этапе конвейера запускается каждый из них?
29. В чем разница между черным, белым и серым ящиком при проведении тестирования на проникновение?
30. Как работает интерактивное тестирование безопасности приложений (IAST) и какие данные оно предоставляет разработчику?
31. Опишите полный цикл управления уязвимостями (Vulnerability Management) от получения уведомления о CVE до установки патча.
32. Что такое Hardening (безопасное конфигурирование) сервера и какие базовые действия он включает?
33. Назовите три ключевых заголовка безопасности HTTP (например, CSP, HSTS) и объясните, от чего они защищают.
34. Каковы требования к логированию событий безопасности согласно общепринятым стандартам (например, PCI DSS или NIST)?

35. Что такое «безопасный по умолчанию» (Secure by Default) конфиг и почему он важен при релизе?
36. Из каких основных этапов состоит цикл безопасной разработки (SDL) и как он накладывается на стандартный Agile/DevOps?
37. Как распределяются задачи по безопасности в методологиях DevSecOps?
38. Что такое метрика MTTD (Mean Time To Detect) и как она рассчитывается в контексте безопасности приложений?
39. Что такое метрика MTTR (Mean Time To Remediate) и от каких факторов зависит скорость устранения уязвимостей?
40. Назовите три ключевые метрики эффективности процесса безопасной разработки, помимо MTTD и MTTR.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Васильева Е. Н. Угрозы безопасности информационных технологий. / [Электронный ресурс]: учеб. пособие / Е.Н. Васильева, В.В. Цехановский, 2005. - 63 с.

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557

3. Основы защиты информации в современных информационных системах: учебное пособие / Н. Ю. Бабанов, А. А. Евстифеев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2022. — 175 с. — ISBN 978-5-9515-0491-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132622.html

4. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

5. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

6. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва: Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Доступ ЭБС «Консультант студента».

7. Павловская, Т. А. Программирование на языке высокого уровня C# : учебное пособие / Т. А. Павловская. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 245 с. — ISBN 978-5-4497-0862-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/146386.html. — Режим доступа: для авторизир. Пользователей.

7.2. Дополнительная литература

1. Скулкин, О. Шифровальщики : как реагировать на атаки с использованием программ- вымогателей : [16+] / О. Скулкин ; науч. ред. А. Алексеев ; ред. К. Ахметов ; пер. с англ. А. Власюк. – Москва : Альпина Паблишер, 2023. – 205 с. : ил. – Режим доступа: по подписке. – URL:https://biblioclub.ru/index.php?page=book&id=707831. – ISBN 978-5-206-00080-1. – Текст : электронный.

2. Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия [Электронный ресурс]: курс/ О. Р. Лапонина. - 2-е изд., исправ. - Москва: ИНТУИТ, 2016. - 462 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429094

3. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

4. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Научная электронная библиотека - http://elibrary.ru/;
8. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
9. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;
10. Безопасность - http://groteck.ru/security.
11. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining Васильев В. И., Вульфин А. М., Кириллова А.Д., Кучкарова Н. В. URL:Glava2/Index1.phphttps://sccs.intelgr.com /archive/2021-03/04-Vasilyev.pdf

12. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации Барабанов А.В., ФедичевА.В. https://cyberleninka.ru/article/n/razrabotka-tipovoymetodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-provedenii-sertifikatsionnyh-ispytaniy-po-trebovaniyam/viewer

13. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ).

13. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ)

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Безопасная разработка программного обеспечения»

образовательной программы высшего образования –
программы специалитета

10.05.03 Информационная безопасность автоматизированных систем
Специализация №5 "Безопасность открытых информационных систем"

Трудоемкость дисциплины: 4 з.е. (144 академических часа – очная форма обучения)

Семестр: 11 (очная форма обучения)

Курс: 6 (очная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Введение в безопасную разработку и нормативная база. Моделирование угроз и проектирование архитектуры безопасности. Безопасная разработка исходного кода. Управление сторонними компонентами и цепочкой поставок. Безопасная сборка, хранение артефактов и управление секретами. Тестирование на проникновение и динамический анализ. Безопасный релиз, эксплуатация и реагирование на инциденты. Внедрение SDL (Secure Development Lifecycle).

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины
«Безопасная разработка программного обеспечения»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.