**МИНОБРНАУКИ РОССИИ**
**федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Самарский государственный технический университет»**
**(ФГБОУ ВО «СамГТУ»)**

УТВЕРЖДАЮ:
Проректор по учебной работе

_____
(подпись, ФИО)
«____»_____20__ г.

# РАБОЧАЯ ПРОГРАММА МОДУЛЯ

## Обеспечение безопасности web-приложений

| | |
|---|---|
| **УГСН** | 09.00.00 Информатика и вычислительная техника |
| **Направление подготовки (специальность)** | 09.03.01 Информатика и вычислительная техника |
| **Квалификация** | *Бакалавр* |
| **Форма обучения** | *Очная* |
| **Год начала подготовки** | *2026* |
| **Объем дисциплины, ч. / з.е. / недели** | *108/3/2* |
| **Образовательные технологии** | *Традиционные* |
| **Форма контроля (промежуточная аттестация)** | *Семестр 1: Экзамен* |
| **Подразделение – разработчик** | *Кафедра «Информатика и вычислительная техника»* |

**Самара 2026**

***Обеспечение безопасности web-приложений***

Разработчик

| |
|---|
| Разработчик РПМ |
| Золин Алексей Георгиевич |
| Руководитель подразделения |
| Чуваков Александр Владимирович |

**СОДЕРЖАНИЕ**

**1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы 3**

**2. Место модуля в структуре образовательной программы 3**

**3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 4**

**4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5**

4.1. Содержание лекционных занятий 6

4.2. Содержание лабораторных занятия 7

4.3. Содержание практических занятий 8

4.4. Содержание самостоятельной работы 9

**5. Перечень учебной литературы и учебно-методического обеспечения по модулю 9**

**6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10**

**7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю 10**

**ПРИЛОЖЕНИЕ 11**

**Фонд оценочных средств 11**

**1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы**

*Таблица 1*

| **Наименование категории (группы) компетенций** | **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Результаты обучения** (знать, уметь, владеть) |
|---|---|---|---|
| **Профессиональные компетенции** | | | |
| - | ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению | ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных продуктов, технических средств | Знать методы и приемы формализации задач. |
| | | ПК-1.2 Знает методологии и технологии проектирования и использования баз данных, разработки компьютерного программного обеспечения и технологии программирования | Знать методологии и технологии проектирования баз данных. |
| | | ПК-1.3 Использует методы и средства проектирования программного обеспечения, структур и баз данных, существующие типовые решения и шаблоны проектирования компьютерного программного обеспечения | Уметь применять средства проектирования программного обеспечения. |
| | | ПК-1.4 Проектирует структуры данных, баз данных, владеет сбором, систематизацией, выявлением взаимосвязей и документированием требований к компьютерному программному обеспечению | Владеть проектированием баз данных. |
| - | ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию | ПК-6.5 Владеет применением методов тестирования при выявлении и описании отклонений работы системы от требований | Владеть навыками тестирования систем. |

### *2. Место модуля в структуре образовательной программы*

Модуль входит в Вариативную часть.

Входные требования:

*Предшествующие осваиваемые модули*: Разработка WEB приложений, Разработка мобильных приложений для Android, Методы и технологии искусственного интеллекта, Язык программирования Python, Язык программирования JavaScript, Язык программирования Java, Нереляционные системы хранения данных, Практико-ориентированный проект, Системный анализ и объектно-ориентированное проектирование, Язык программирования C#, Математическое и имитационное моделирование, Производственная практика: преддипломная практика, Цифровая экономика, UI/UX дизайн, Разработка программного обеспечения экономических систем, Производственная практика: технологическая (проектно-технологическая) практика;

### 3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

*Таблица 3*

| Вид учебной работы | Всего часов | В том числе часов в электронной форме | В том числе часов в форме практической подготовки | Семестр 1 часов/часов в электронной форме/в форме практической подготовки |
|---|---|---|---|---|
| **Аудиторная контактная работа (всего),** в том числе: | **48** | **0** | **0** | **48** |
| лекционные занятия (ЛЗ) | 16 | 0 | 0 | 16 |
| лабораторные работы (ЛР) | 32 | 0 | 0 | 32 |
| практические занятия (ПЗ) | 0 | 0 | 0 | 0 |
| **Внеаудиторная контактная работа, КСР** | **3** | **0** | **0** | **3** |
| **Самостоятельная работа (всего),** в том числе: | **57** | **0** | **0** | **57** |
| Подготовка к лабораторным работам | *47* | *0* | *0* | *47* |
| Подготовка к экзамену | *10* | *0* | *0* | *10* |
| **ИТОГО: час.** | **108** | **0** | **0** | **108** |
| **ИТОГО: з.е.** | **3.0** | **0.0** | **0.0** | **3.0** |

### 4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

*Таблица 4*

| № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, часы | | | | |
|---|---|---|---|---|---|---|
| | | ЛЗ | ЛР | ПЗ | СРС | Всего часов |
| 1. | Информационная безопасность: основные понятия. | 4 | 8 | 0 | 18 | 30 |
| 2. | Анализ угроз Web-приложениям. | 4 | 8 | 0 | 18 | 30 |
| 3. | Методы защиты Web-приложений. | 8 | 16 | 0 | 21 | 45 |

| № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, часы | | | | |
|---|---|---|---|---|---|---|
| | | ЛЗ | ЛР | ПЗ | СРС | Всего часов |
| | **КСР** | | | | | *3* |
| **Итого:** | | *16* | *32* | *0* | *57* | *108* |

### 4.1. Содержание лекционных занятий

*Таблица 4.1*

| № ЛЗ | Наименование раздела | Тема лекции | Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов | Количество часов в электронной форме |
|---|---|---|---|---|---|
| **Семестр 1** | | | | | |
| 1. | Информационная безопасность: основные понятия. | Основные понятия информационной безопасности. | Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности и критической информационной инфраструктуры. | 2 | 0 |
| 2. | Информационная безопасность: основные понятия. | Основные понятия и определения сетевых технологий. | Основные понятия и определения сетевых технологий, используемых в Веб-приложениях. | 2 | 0 |
| 3. | Анализ угроз Web-приложениям. | Структура современных веб-приложений. | REST API. Формат JSON. JavaScript. Программный интерфейс DOM браузера. Фреймворки для SPA. Системы аутентификации и авторизации. Базы данных на стороне сервера. Хранение данных на стороне клиента. | 2 | 0 |
| 4. | Анализ угроз Web-приложениям. | Возможные варианты взлома веб-приложений. | Межсайтовый скриптинг. Подделка межсайтовых запросов. Атака на внешние сущности XML. Внедрение кода. Отказ в обслуживании. Атаки на данные и объекты. Атаки на стороне клиента. Эксплуатация сторонних зависимостей. | 2 | 0 |
| 5. | Методы защиты Web-приложений. | Безопасная архитектура приложений. | Безопасная архитектура приложений. Безопасная конфигурация приложений. Безопасность пользовательского интерфейса. Моделирование угроз. | 2 | 0 |
| 6. | Методы защиты Web-приложений. | Проверка безопасности кода. | Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями. | 2 | 0 |
| 7. | Методы защиты Web-приложений. | Противодействие атакам. | Защита от CSRF. Защита от XXE-атак. Противодействие внедрению. Противодействие DoS-атакам. Противодействие XSS-атакам. | 2 | 0 |
| 8. | Методы защиты Web-приложений. | Защита данных и объектов. | Защита данных и объектов. Защита от атак на стороне клиента. Защита сторонних зависимостей. | 2 | 0 |
| | | | **Итого за семестр:** | *16* | *0* |
| | | | **Итого:** | **16** | **0** |

### 4.2. Содержание лабораторных занятий

*Таблица 4.2*

| № ЛабЗ | Наименование раздела | Наименование лабораторной работы | Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов) | Количество часов | Количество часов в электронной форме | Количество часов в форме практической подготовки |
|---|---|---|---|---|---|---|
| **Семестр 1** | | | | | | |
| 1. | Информационная безопасность: основные понятия. | Основные понятия в области кибербезопасности. | Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности. | 4 | 0 | *0* |
| 2. | Информационная безопасность: основные понятия. | Понятия и определения сетевых технологий. | Работа с протоколами HTTP, HTTPS. Анализ входящего/исходящего трафика. Использование сетевых утилит. | 4 | 0 | *0* |
| 3. | Анализ угроз Web-приложениям. | Структура веб-приложения. | Работа с DOM браузера. Построение простого REST API на стороне сервера. | 4 | 0 | *0* |
| 4. | Анализ угроз Web-приложениям. | Анализ возможности взлома веб-приложений. | Анализ атак на стороне клиента. Анализ атак на стороне сервера. | 4 | 0 | *0* |
| 5. | Методы защиты Web-приложений. | Безопасная архитектура приложений. | Разработка безопасной конфигурации приложений. Обеспечение безопасности пользовательского интерфейса. | 4 | 0 | *0* |
| 6. | Методы защиты Web-приложений. | Обнаружение уязвимостей веб-приложения. | Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями. | 4 | 0 | *0* |
| 7. | Методы защиты Web-приложений. | Противодействие атакам. | Противодействие DoS-атакам. Противодействие XSS-атакам. Противодействие внедрению. | 4 | 0 | *0* |
| 8. | Методы защиты Web-приложений. | Защита данных и объектов. | Защита данных и объектов. Защита от атак на стороне клиента. Защита от атак на стороне сервера. | 4 | 0 | *0* |
| | | | **Итого за семестр:** | *32* | *0* | *0* |
| | | | **Итого:** | **32** | **0** | ***0*** |

### 4.3. Содержание самостоятельной работы

*Таблица 4.4*

| Наименование раздела | Вид самостоятельной работы | Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов |
|---|---|---|---|
| **Семестр 1** | | | |
| Информационная | Подготовка к экзамену | Основные понятия в области кибербезопасности; | 3 |

| Наименование раздела | Вид самостоятельной работы | Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов |
|---|---|---|---|
| безопасность: основные понятия. | | основные угрозы, риски и уязвимости в сфере кибербезопасности. | |
| Информационная безопасность: основные понятия. | Подготовка к лабораторным работам | Изучение основных понятий в области кибербезопасности. | 15 |
| Анализ угроз Web-приложениям. | Подготовка к лабораторным работам | Изучение основных угроз веб-приложениям. | 15 |
| Анализ угроз Web-приложениям. | Подготовка к экзамену | Изучение основных типов веб-приложений. Изучение основных угроз веб-приложениям. | 3 |
| Методы защиты Web-приложений. | Подготовка к лабораторным работам | Изучение методов защиты от основных атак на веб-приложения. | 17 |
| Методы защиты Web-приложений. | Подготовка к экзамену | Изучение методов защиты от основных атак на веб-приложения. | 4 |
| | | **Итого за семестр:** | *57* |
| | | **Итого:** | **57** |

## 5. Перечень учебной литературы и учебно-методического обеспечения по модулю

*Таблица 5*

| № п/п | Библиографическое описание | Ресурс НТБ СамГТУ | Ссылка на ресурс |
|---|---|---|---|
| 1. | Краковский, Ю.М. Информационная безопасность и защита информации : Учеб.пособие / Ю. М. Краковский.- М., МарТ, 2008.- 287 с. | Книжный фонд СамГТУ | http://platform.samgtu.ru/getinfo?uid=els_samgtu-catalog-103315 |
| 2. | Ворожейкин, В.Н. Технические средства и методы защиты информации – дополнительные главы : Лабораторный практикум / В. Н. Ворожейкин; Самар.гос.техн.ун-т, Электронные системы и информационная безопасность .- 2-е изд..- Самара, 2019.- 336 с. | Электронная библиотека СамГТУ (ЭБС Политех) | http://platform.samgtu.ru/getinfo?uid=els_samgtu-elib-3574 |
| 3. | Кибербезопасность в условиях электронного банкинга; Прометей, 2020 | ЭБС IPR Books | http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-125665 |
| 4. | Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения; Техносфера, 2021 | ЭБС IPR Books | http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-108023 |
| 5. | Информационная безопасность и защита информации; Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014 | ЭБС IPR Books | http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-43183 |
| 6. | Кибероружие и кибербезопасность. О сложных вещах простыми словами; Инфра-Инженерия, 2025 | ЭБС IPR Books | http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-154736 |
| 7. | Прохорова, Ольга Витольдовна Информационная безопасность и защита информации : учеб. [для 2 курса специальности 230400.62 "Информ. системы и технологии"] [Текст] / Самар. гос. архитектур.-строит. ун-т (СГАСУ), Каф. приклад. математики и вычисл. техники.- Самара, СГАСУ, 2014.- 112 с.: ил. | Книжный фонд АСА СамГТУ | http://platform.samgtu.ru/getinfo?uid=els_samgtu-asa-71304 |

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

## 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

*Таблица 6*

| № п/п | Наименование | Ссылка на веб-страницу ресурса | Режим доступа |
|---|---|---|---|
| 1. | *Scopus: база данных рефератов и цитирования [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет* | *http://www.scopus.com* | *Ресурсы ограниченного доступа* |
| 2. | *Библиотека компьютерной литературы [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет* | *http://it.eup.ru/* | *Ресурсы открытого доступа* |

## 7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю

**Лекционные занятия** проводятся в:
Учебная аудитория.

**Практические занятия** не предусмотрены.

**Самостоятельная работа** проводятся в:
Корпус № 8/200 - Читальный зал (Аудитория на 70 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные.).

**Лабораторные занятия** проводятся в:
Корпус № 8/419 - Компьютерный класс (Аудитория на 33 посадочных места оснащена следующими техническими средствами обучения и оборудованием: парты, столы учебные, доска аудиторная магнитно-маркерная 100х180 эмаль. 12 ПК LG FLATRON 22EN43 в комплекте. На ПК, на базе операционной системы MS Windows 7 Professional, установлено следующее ПО: офисный пакет MS Office 2007, Oracle VirtualBox, K-LiteCodecPack, Far Manager, 7-Zip,Notepad++, Foxit Reader, PostgreSQL, Google Chrome, OpenJDK, Apache NetBeans, PVS-Studio, Microsoft Visual Studio, Microsoft SQL Server 2012, Microsoft SQL Server Managment Studio, Kaspersky Endpoint Security, Microsoft Office Project Профессиональный 2007, MATLAB R2010a, Scilab-6.0.1 (64bit), Microsoft Visio Профессиональный 2010, Microsoft .NET Framework 4.8, Android Studio, Mozilla Firefox 68.0.2 (64 ru), Deductor Academic. Обеспечено проводное подключение ПК к локальной сети и сети Интернет.)

Корпус № 8/422 - Компьютерный класс (Аудитория на 34 посадочных места оснащена следующими техническими средствами обучения и оборудованием: парты, столы учебные, доска аудиторная магнитно-маркерная 100х180 эмаль, проектор Optome EX551; 1 ПК Intel Core i5 в комплекте, 10 ПК AMD Ruzen 5 5600G OEM. На базе операционной системы MS Windows 7 Professional на ПК установлены следующие ПО: офисный пакет MS Office 2007, Oracle VirtualBox, K-LiteCodecPack, Far Manager, 7-Zip,Notepad++, Foxit Reader, PostgreSQL, Google Chrome, OpenJDK, Apache NetBeans, PVS-Studio, Microsoft Visual Studio, Microsoft SQL Server 2012, Microsoft SQL Server Managment Studio, Kaspersky Endpoint Security, Microsoft Office Project Профессиональный 2007, MATLAB R2010a, Scilab-6.0.1 (64bit), Microsoft Visio Профессиональный 2010, Microsoft .NET Framework 4.8, Android Studio, Mozilla Firefox 68.0.2 (64 ru), Deductor Academic. Обеспечено проводное подключение ПК к локальной сети и сети Интернет.)

Корпус № 8/414 - Компьютерный класс (Аудитория на 36 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная магнитно-маркерная, 1 персональный компьютер iRU 320 FX-4100/Gigabyte Ga-880GMA-USB3/4Gb/320Gb/k+M/DVDRW, с операционной системой Microsoft Windows 7 Professional. На ПК установлены ПО: Oracle VirtualBox, K-LiteCodecPack, Far Manager, 7-Zip,Notepad++, Foxit Reader, PostgreSQL, Google Chrome, OpenJDK, Apache NetBeans, PVS-Studio, Microsoft Visual Studio, Microsoft SQL Server 2012, Microsoft SQL Server Managment Studio, Kaspersky Endpoint Security, Microsoft Office Project Профессиональный 2007, MATLAB R2010a, Scilab-6.0.1 (64bit), Microsoft Visio Профессиональный 2010, Microsoft .NET Framework 4.8, Android Studio, Mozilla Firefox 68.0.2 (64 ru), Deductor Academic. 9 ПК Intel Core i5 с операционной системой Microsoft Windows 7 Professional. На ПК установлены ПО: офисный пакет MS Office 2007, Oracle VirtualBox, K-LiteCodecPack, Far Manager, 7-Zip,Notepad++, Foxit Reader, PostgreSQL, Google Chrome, OpenJDK, Apache NetBeans, PVS-Studio, Microsoft Visual Studio, Microsoft SQL Server 2012, Microsoft SQL Server Managment Studio, Kaspersky Endpoint Security, Microsoft Office Project Профессиональный 2007, MATLAB R2010a, Scilab-6.0.1 (64bit), Microsoft Visio Профессиональный 2010, Microsoft .NET Framework 4.8, Android Studio, Mozilla Firefox 68.0.2 (64 ru), Deductor Academic. Обеспечено проводное подключение ПК к локальной сети и сети Интернет.).

ПРИЛОЖЕНИЕ

**Фонд оценочных средств**

**Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации обучающихся по модулю**

Настоящий Фонд оценочных средств (ФОС) по модулю Обеспечение безопасности web-приложений является неотъемлемым приложением к рабочей программе модуля. На данный ФОС распространяются все реквизиты утверждения, представленные в рабочей программе модуля.

**1. Перечень оценочных средств**

*Таблица 1*

| № п/п | Оценочное средство | Краткая характеристика оценочного средства | Количество | Представление оценочного средства в ФОС |
|---|---|---|---|---|
| 1 | Устный (письменный) опрос | Диалог преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала. | 3 | Перечень вопросов для обсуждения |
| 2 | Отчёт по лабораторной работе | Оценка способности студента применить полученные ранее знания для проведения анализа, опыта, эксперимента и выполнения последующих расчетов, а также составления выводов. | 8 | Требования к содержанию и оформлению отчета |
| 3 | Контрольная точка в форме контрольной работы | Средство рубежного контроля остаточных знаний и умений, обычно состоящее из нескольких вопросов или заданий, которые студент должен решить, выполнить. | 4 | Пример варианта контрольной работы |

**Раздел 2. Этапы формирования компетенций, соотнесенные с видами оценочных средств**

*Таблица 2*

| Контролируемые разделы модуля | Код и формулировка индикатора компетенции | Результат обучения | Оценочные средства | Номер оценочного средства |
|---|---|---|---|---|
| Информационная безопасность: основные понятия. | ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных продуктов, технических средств | Знать методы и приемы формализации задач. | Устный (письменный) опрос | 1 |
| Информационная безопасность: основные понятия. | ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных | Знать методы и приемы формализации задач. | Отчёт по лабораторной работе | 1-2 |

| Контролируемые разделы модуля | Код и формулировка индикатора компетенции | Результат обучения | Оценочные средства | Номер оценочного средства |
|---|---|---|---|---|
| | продуктов, технических средств | | | |
| Информационная безопасность: основные понятия. | ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных продуктов, технических средств | Знать методы и приемы формализации задач. | Контрольная точка в форме контрольной работы | 1 |
| Анализ угроз Web-приложениям. | ПК-1.2 Знает методологии и технологии проектирования и использования баз данных, разработки компьютерного программного обеспечения и технологии программирования | Знать методологии и технологии проектирования баз данных. | Устный (письменный) опрос | 2 |
| Анализ угроз Web-приложениям. | ПК-1.3 Использует методы и средства проектирования программного обеспечения, структур и баз данных, существующие типовые решения и шаблоны проектирования компьютерного программного обеспечения | Уметь применять средства проектирования программного обеспечения. | Отчёт по лабораторной работе | 3-4 |
| Анализ угроз Web-приложениям. | ПК-1.4 Проектирует структуры данных, баз данных, владеет сбором, систематизацией, выявлением взаимосвязей и документированием требований к компьютерному программному обеспечению | Владеть проектированием баз данных. | Контрольная точка в форме контрольной работы | 2 |
| Методы защиты Web-приложений. | ПК-1.2 Знает методологии и технологии проектирования и использования баз данных, разработки компьютерного программного обеспечения и технологии программирования | Знать методологии и технологии проектирования баз данных. | Устный (письменный) опрос | 3 |
| Методы защиты Web-приложений. | ПК-1.3 Использует методы и средства проектирования программного обеспечения, структур и баз данных, | Уметь применять средства проектирования программного обеспечения. | Отчёт по лабораторной работе | 5-8 |

| Контролируемые разделы модуля | Код и формулировка индикатора компетенции | Результат обучения | Оценочные средства | Номер оценочного средства |
|---|---|---|---|---|
| | существующие типовые решения и шаблоны проектирования компьютерного программного обеспечения | | | |
| Методы защиты Web-приложений. | ПК-1.4 Проектирует структуры данных, баз данных, владеет сбором, систематизацией, выявлением взаимосвязей и документированием требований к компьютерному программному обеспечению | Владеть проектированием баз данных. | Контрольная точка в форме контрольной работы | 3-4 |

**3. Содержание оценочных средств текущего контроля**

| |
|---|
| Оценочное средство 1: |
| Перечень вопросов для устного опроса прикреплен в файле. |
| Оценочное средство 2: |
| Шаблон отчета по Лабораторным работам прикреплен в файле. |
| Оценочное средство 3: |
| Задания на контрольные работы прикреплены в файле. |

**4. Содержание оценочных средств промежуточной аттестации**

Семестр 1:

Вид аттестационного испытания 1: Устное собеседование.
Форма проведения промежуточной аттестации: Экзамен.
Типовые задания: .

**5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций**

Модуль состоит из набора разделов. Объем учебного раздела раскрывает отдельную (ые) тему(ы) модуля / этап прохождения практики. Модуль разбивается, как правило, на 2-4 раздела в семестр.

Раздел состоит из учебных элементов (дидактических единиц), сгруппированных по темам в рамках раздела. Объем учебного материала учебного элемента раскрывает отдельный вопрос темы. Путем набора соответствующих тем и учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

По каждому разделу устанавливается перечень обязательных видов работы студента, включающий: ответы на теоретические вопросы на семинаре; решение практических задач и выполнение заданий на практических занятиях; выполнение лабораторных работ; выполнение контрольных работ; написание рефератов; участие в коллоквиумах; тестирование по теме (группе тем); другие виды работ, определяемые преподавателем (в соответствии с установленными требованиями балльно-рейтинговой технологии).

Каждый раздел включает определенные формы контроля для оценки уровня усвоения учебного материала и определения рейтинговой оценки качества усвоения учебного материала.

Рейтинговая оценка знаний студентов определяется по 100-балльной шкале в каждом семестре и включает текущий, рубежный и итоговый контроль.

**Накопленный рейтинг** (фиксированная величина по окончании семестра) — это фактический рейтинг по всем освоенным к данному моменту разделам дисциплины, включая их текущий, рубежный и итоговый контроль, составляет N баллов (N – индивидуальная величина, зависящая от проделанной работы студента по дисциплине).

**Проходной рейтинг** (включает текущий контроль, рубежный контроль в семестре и промежуточную аттестацию) — это минимум баллов, набрав который студент будет считаться аттестованным по дисциплине, составляет 60 баллов в семестр по одной дисциплине.

**Пороговый рейтинг** (включает текущий контроль и рубежный контроль в семестре) — это минимальный фактический рейтинг семестрового контроля, набрав который, студент проходит на итоговый контроль, составляет 50% от суммы баллов, которые студент может набрать за текущий контроль и рубежный контроль в течение семестра.

**Текущий контроль** служит для получения первичной информации о ходе усвоения отдельных элементов содержания учебной дисциплины. Основное его назначение состоит в осуществлении контроля за всеми видами аудиторной и самостоятельной внеаудиторной деятельности студентов, результаты которого оцениваются в баллах.

**Рубежный контроль** (контрольные точки текущего контроля) проводится после изучения завершенной в смысловом и логическом плане части учебного материала (раздела, модуля). Этот вид контроля позволяет получить информацию о ходе усвоения некоторой совокупности содержательных элементов учебной дисциплины (раздела, модуля) и оценивается в баллах.

**Промежуточный итоговый контроль** (контрольные точки промежуточной аттестации) – курсовой проект, курсовая работа и экзамен, зачет, зачет с оценкой. Итоговый контроль по дисциплине в семестре предназначен для аттестации студента по учебной дисциплине: процедура установления соответствия уровня и качества подготовки студентов системе требований, зафиксированной в ФГОС ВО.

**Распределение баллов рейтинговой оценки между видами контроля**

*Таблица 3*

| Номер семестра | Распределение баллов | | | | | Проходной рейтинг |
|---|---|---|---|---|---|---|
| | Текущий и рубежный контроль | | | Промежуточный итоговый контроль | | |
| | Текущий контроль | Рубежный контроль | Пороговый рейтинг | Курсовая работа/курсовой проект | Зачет/зачет с оценкой/экзамен | |
| 1 | 48 | 22 | 35 | 0 | 30 | 60 |

**Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации**

*Таблица 4*

| | | | | |
|---|---|---|---|---|
| 100-балльная шкала | 85-100 | 75-84 | 60-74 | 0-59 |
| 5-балльная шкала | Отлично | Хорошо | Удовлетворительно | Неудовлетворительно |
| Бинарная шкала | Зачтено | | | Не зачтено |

Распределение рейтинговых баллов по разделам модуля с указанием применяемых для их начисления оценочных средств представлено в Технологической карте БРТ.

**Технологическая карта БРТ**

*Семестр 1*

| Раздел учебного модуля | Оценочные средства | | | | Итого |
|---|---|---|---|---|---|
| | **Устный (письменный) опрос** | **Отчёт по лабораторной работе** | **Контрольная точка в форме контрольной работы** | **Экзамен** | |
| Раздел 1 | | | | | |
| ЛР 1.1 | 5 | 5 | 0 | | 10 |
| ЛР 1.2 | 0 | 5 | 5 | | 10 |
| Итого по разделу 1 | 5 | 10 | 5 | | 20 |
| Раздел 2 | | | | | |
| ЛР 2.3 | 5 | 5 | 0 | | 10 |
| ЛР 2.4 | 0 | 5 | 5 | | 10 |
| Итого по разделу 2 | 5 | 10 | 5 | | 20 |
| Раздел 3 | | | | | |
| ЛР 3.5 | 2 | 4 | 6 | | 12 |
| ЛР 3.6 | 0 | 4 | 0 | | 4 |
| ЛР 3.7 | 0 | 4 | 0 | | 4 |
| ЛР 3.8 | 0 | 4 | 6 | | 10 |
| Итого по разделу 3 | 2 | 16 | 12 | | 30 |
| Промежуточная аттестация | | | | 30 | 30 |
| Итого | 12 | 36 | 22 | 30 | 100 |

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Институт автоматики и информационных технологий

Кафедра «Информатика и вычислительная техника»

# О Т Ч Е Т

о выполнении лабораторной работы №

Наименование лабораторной работы

по дисциплине «Наименование дисциплины»

Вариант № (при наличии)

**Преподаватель**

| *(должность)* | *(подпись)* | *(дата)* | *(инициалы, фамилия)* |
|---|---|---|---|

**Преподаватель**

| *(должность)* | *(подпись)* | *(дата)* | *(инициалы, фамилия)* |
|---|---|---|---|

**Студент**

| *(группа)* | *(подпись)* | *(дата)* | *(инициалы, фамилия)* |
|---|---|---|---|

Самара 20__ г.

**Цель работы:**

Приводится цель работы.

**Задачи работы:**

- приводятся задачи по изучению материала, решаемые при выполнении работы.

**Задание 1 «Наименование задания»**

Текст задания…

Приводится по этапное решение задания (код, математические вычисления, графики и т.д.)

Результаты работы программы

**Выводы**

**Задание 2 (если есть)**

Текст задания…

Приводится по этапное решение задания (код, математические вычисления, графики и т.д.)

Результаты работы программы

**Выводы**

## Вопросы к экзамену

1. Что такое объектная модель документа (DOM)?
2. Какое основное назначение DOM?
3. Какие методы используются для изменения элементов страницы?
4. Чем отличается innerHTML от createElement()?
5. Объясните разницу между `getElementsByClassName()` и `querySelectorAll()`.
6. Что такое событие в JavaScript и как оно обрабатывается?
7. Назовите наиболее распространенные события в браузере.
8. Опишите процесс обработки событий на примере клика мыши.
9. Как добавить обработчик события элементу?
10. Почему важно правильно удалять элементы и события в DOM?
11. Что означает аббревиатура REST?
12. Перечислите базовые принципы архитектуры REST.
13. Каковы преимущества использования RESTful сервисов перед SOAP?
14. Какой тип HTTP-запросов используется для чтения ресурсов?
15. Какой метод применяется для обновления ресурса?
16. Как создать новый ресурс через REST API?
17. Для чего нужен HTTP-код состояния 200 OK?
18. Приведите пример простейшего REST-запроса на создание нового объекта.
19. Объясните принцип взаимодействия клиент-сервер через REST.
20. Чем отличаются GET и POST запросы в REST API?
21. Что такое межсайтовое выполнение скриптов (XSS)?
22. Какие типы XSS существуют?
23. Опасность внедрения произвольного HTML-кода в страницу сайта.
24. Что значит CSRF и почему эта атака опасна?
25. Основные способы защиты от XSS.
26. Роль Content Security Policy (CSP).
27. Почему важна проверка ввода и вывод данных пользователями?
28. Как браузер защищает пользователей от атак типа Clickjacking?
29. Описать атаку Session Fixation.
30. Методы предотвращения атаки CSRF.
31. Что такое SQL-инъекция и как она работает?
32. Примеры SQL-инъекции.
33. Что такое Remote Code Execution (RCE)?
34. Как защититься от инъекций команд оболочки (Shell Injection)?
35. Особенности Directory Traversal Attacks.
36. Почему защита сессий критична для веб-приложений?
37. Возможности атаки на сервер путем злоупотребления доступом к файлам.
38. Способы защиты от переполнения буфера.
39. Зачем проводить аудит исходного кода приложения?
40. Принцип ограничения привилегий и минимальных прав.
41. Дайте определение понятию "угроза кибербезопасности".
42. Чем риск отличается от угрозы?
43. В чём заключается понятие "уязвимость"?
44. По каким признакам классифицируются киберугрозы?
45. Назовите известные виды угроз информационной безопасности.
46. Что такое DDoS-атака и её последствия?
47. Охарактеризуйте атаки класса Man-in-the-Middle (MITM).
48. Понятие Phishing и его опасность.
49. Чем Malware отличается от Virus?
50. Объяснить роль двухфакторной аутентификации (2FA).
51. Отличия протокола HTTP от HTTPS.

52. Как устроены заголовки HTTP-запросов?
53. Кратко опишите работу SSL/TLS.
54. Какие алгоритмы шифрования применяются в HTTPS?
55. Чем полезен механизм cookie?
56. Назначение токенов сессии (session tokens).
57. Расскажите о принципе работы метода POST.
58. Что означают коды статуса 301 и 302?
59. Какие проблемы связаны с передачей данных открытым текстом?
60. Может ли HTTPS защитить от всех видов атак?
61. Что представляет собой трафик сети Интернет?
62. Какие инструменты позволяют анализировать трафик?
63. Расшифруйте значение Wireshark.
64. Назовите основные категории сетевого анализа.
65. Что позволяет увидеть инструмент tcpdump?
66. Объясните смысл сниффинга пакетов.
67. Зачем нужны прокси-серверы?
68. Применение VPN для повышения безопасности.
69. Как работает технология Deep Packet Inspection (DPI)?
70. Чем полезна фильтрация на уровне протоколов?
71. Какие меры предосторожности необходимы при настройке веб-приложения?
72. Важность настройки secure cookies.
73. Что включает в себя настройка механизма аутентификации?
74. Причины отказа от использования слабых паролей.
75. Зачем реализовывать защиту от брутфорс-атак?
76. Когда целесообразно использование CAPTCHA?
77. Методики проверки подлинности запросов.
78. Значение системы контроля версий (VCS) для безопасности.
79. Оптимальные практики управления ключами шифрования.
80. Преимущества своевременного обновления библиотек и фреймворков.
81. Важность валидаторов формы.
82. Пользовательские подсказки о защите аккаунта.
83. Необходимость ограничений скорости отправки форм.
84. Правильная реализация уведомлений об ошибках регистрации.
85. Реализация надежных механизмов восстановления пароля.
86. Использование статического анализа UI-компонентов.
87. Как предотвратить отображение конфиденциальных данных в интерфейсе?
88. Как избежать информирования злоумышленников об успешности попыток взлома?
89. Инструменты автоматизации тестирования пользовательских интерфейсов.
90. Зачем настраивать строгую политику паролей?
91. Цели процесса выявления уязвимостей.
92. Какова роль автоматизированных инструментов сканирования кода?
93. Подходы к обнаружению уязвимых зависимостей.
94. Как организовать регулярное тестирование безопасности приложений?
95. Чем полезны динамические тесты (Dynamic Application Security Testing, DAST)?
96. Что входит в процесс Patch Management?
97. Чем Static Analysis Security Testing (SAST) отличается от Dynamic Analysis?
98. Чем является уязвимость нулевого дня (Zero-day vulnerability)?
99. В чём отличие периодической оценки рисков от постоянного мониторинга?
100. Какие стандарты применяют для классификации уязвимостей?
101. Суть DoS-атаки и её отличия от DDoS.
102. Признаки обнаружения DoS/DDoS-атаки.

103. Эффективные стратегии борьбы с DDoS-атаками.
104. Полезность распределения нагрузки (Load Balancing).
105. Почему важен мониторинг производительности веб-ресурса?
106. Влияние объема входящего трафика на производительность сервера.
107. Практическое применение CDN-сервисов против DDoS.
108. Способны ли аппаратные фаерволлы противостоять современным DDoS-атакам?
109. Что даёт повышение отказоустойчивости инфраструктуры?
110. Стоит ли применять captcha при подозрительных действиях пользователей?
111. Разновидности XSS-атак.
112. Пример реализации stored-XSS.
113. Чем опасно внедрение JavaScript-вредоносного кода на странице?
114. Основные подходы к предотвращению XSS.
115. Важно ли использовать экранирование символов?
116. Помогут ли фильтры WAF (Web Application Firewall) от XSS?
117. Насколько эффективны контентные правила CSP?
118. Проблемы безопасности при выполнении асинхронных AJAX-запросов.
119. Есть ли связь между использованием устаревших технологий и риском XSS?
120. Нужно ли проверять данные на выходе в дополнение к данным на входе?
121. Типичные примеры SQL-инъекций.
122. Возможность обхода фильтров введённых данных.
123. Основной способ предотвращения инъекции кода.
124. Является ли параметризованный SQL-запрос надежным методом защиты?
125. Причины появления PHP-инъекций.
126. Чем грозит OS Command Injection?
127. Безопасность директорий и файлов в Linux относительно инъекционных атак.
128. Зачем проводится проверка путей файлов (Path Validation)?
129. Правила разработки защищенных шаблонов страниц.
130. Достаточно ли одной проверки входящих данных для полной защиты?
131. Основные технологии шифрования данных.
132. Важность разделения зон ответственности администратора и разработчика.
133. Ключевые моменты в управлении доступом к ресурсам.
134. Механизмы контроля целостности данных.
135. Чем полезно резервирование и восстановление данных?
136. Почему важны контроль версий и управление изменениями (Change Management)?
137. Кто должен иметь права администрирования баз данных?
138. Недостаточность одних лишь мер по защите базы данных.
139. Средства мониторинга активности сотрудников.
140. Основы многоуровневой защиты данных.
141. Почему небезопасно хранить важные данные в локальном хранилище браузера?
142. Проблема утечки данных через JavaScript-файлы сторонних разработчиков.
143. Способы снижения риска утечек персональных данных через Google Analytics.
144. Чем опасны атаки click-jacking и как от них защититься?
145. Нужна ли защита от повторного использования сессии (Session Replay)?
146. Критичность использования предсказуемых временных меток для имен файлов.
147. Последствия отсутствия ограниченного числа неудачных попыток входа.
148. Недостаточная защита при обработке загрузочных файлов.
149. Важность фильтрации заголовков запросов.

150. Защищённость путём отключения ненужных служб и модулей на сервере.

# Вопросы к экзамену

## Вопросы по работе с DOM браузера

1. Что такое объектная модель документа (DOM)?
2. Какое основное назначение DOM?
3. Какие методы используются для изменения элементов страницы?
4. Чем отличается innerHTML от createElement()?
5. Объясните разницу между `getElementsByClassName()` и `querySelectorAll()`.
6. Что такое событие в JavaScript и как оно обрабатывается?
7. Назовите наиболее распространенные события в браузере.
8. Опишите процесс обработки событий на примере клика мыши.
9. Как добавить обработчик события элементу?
10. Почему важно правильно удалять элементы и события в DOM?

## Вопросы по построению простого REST API на стороне сервера

1. Что означает аббревиатура REST?
2. Перечислите базовые принципы архитектуры REST.
3. Каковы преимущества использования RESTful сервисов перед SOAP?
4. Какой тип HTTP-запросов используется для чтения ресурсов?
5. Какой метод применяется для обновления ресурса?
6. Как создать новый ресурс через REST API?
7. Для чего нужен HTTP-код состояния 200 OK?
8. Приведите пример простейшего REST-запроса на создание нового объекта.
9. Объясните принцип взаимодействия клиент-сервер через REST.
10. Чем отличаются GET и POST запросы в REST API?

## Вопросы по анализу атак на стороне клиента и сервере

1. Что такое межсайтовое выполнение скриптов (XSS)?
2. Какие типы XSS существуют?
3. Опасность внедрения произвольного HTML-кода в страницу сайта.
4. Что значит CSRF и почему эта атака опасна?
5. Основные способы защиты от XSS.
6. Роль Content Security Policy (CSP).
7. Почему важна проверка ввода и вывод данных пользователями?
8. Как браузер защищает пользователей от атак типа Clickjacking?
9. Описать атаку Session Fixation.
10. Методы предотвращения атаки CSRF.
11. Что такое SQL-инъекция и как она работает?
12. Примеры SQL-инъекции.
13. Что такое Remote Code Execution (RCE)?
14. Как защититься от инъекций команд оболочки (Shell Injection)?
15. Особенности Directory Traversal Attacks.
16. Почему защита сессий критична для веб-приложений?
17. Возможности атаки на сервер путем злоупотребления доступом к файлам.
18. Способы защиты от переполнения буфера.
19. Зачем проводить аудит исходного кода приложения?
20. Принцип ограничения привилегий и минимальных прав.

**Вопросы по основным понятиям в области кибербезопасности**

1. Дайте определение понятию "угроза кибербезопасности".
2. Чем риск отличается от угрозы?
3. В чём заключается понятие "уязвимость"?
4. По каким признакам классифицируются киберугрозы?
5. Назовите известные виды угроз информационной безопасности.
6. Что такое DDoS-атака и её последствия?
7. Охарактеризуйте атаки класса Man-in-the-Middle (MITM).
8. Понятие Phishing и его опасность.
9. Чем Malware отличается от Virus?
10. Объяснить роль двухфакторной аутентификации (2FA).

**Вопросы по работе с протоколами HTTP и HTTPS**

1. Отличия протокола HTTP от HTTPS.
2. Как устроены заголовки HTTP-запросов?
3. Кратко опишите работу SSL/TLS.
4. Какие алгоритмы шифрования применяются в HTTPS?
5. Чем полезен механизм cookie?
6. Назначение токенов сессии (session tokens).
7. Расскажите о принципе работы метода POST.
8. Что означают коды статуса 301 и 302?
9. Какие проблемы связаны с передачей данных открытым текстом?
10. Может ли HTTPS защитить от всех видов атак?

**Вопросы по анализу входящего/исходящего трафика и сетевым утилитам**

1. Что представляет собой трафик сети Интернет?
2. Какие инструменты позволяют анализировать трафик?
3. Расшифруйте значение Wireshark.
4. Назовите основные категории сетевого анализа.
5. Что позволяет увидеть инструмент tcpdump?
6. Объясните смысл сниффинга пакетов.
7. Зачем нужны прокси-серверы?
8. Применение VPN для повышения безопасности.
9. Как работает технология Deep Packet Inspection (DPI)?
10. Чем полезна фильтрация на уровне протоколов?

**Вопросы по разработке безопасной конфигурации приложений**

1. Какие меры предосторожности необходимы при настройке веб-приложения?
2. Важность настройки secure cookies.
3. Что включает в себя настройка механизма аутентификации?
4. Причины отказа от использования слабых паролей.
5. Зачем реализовывать защиту от брутфорс-атак?
6. Когда целесообразно использование CAPTCHA?
7. Методики проверки подлинности запросов.
8. Значение системы контроля версий (VCS) для безопасности.
9. Оптимальные практики управления ключами шифрования.
10. Преимущества своевременного обновления библиотек и фреймворков.

**Вопросы по обеспечению безопасности пользовательского интерфейса**

1. Важность валидаторов формы.
2. Пользовательские подсказки о защите аккаунта.
3. Необходимость ограничений скорости отправки форм.
4. Правильная реализация уведомлений об ошибках регистрации.
5. Реализация надежных механизмов восстановления пароля.
6. Использование статического анализа UI-компонентов.
7. Как предотвратить отображение конфиденциальных данных в интерфейсе?
8. Как избежать информирования злоумышленников об успешности попыток взлома?
9. Инструменты автоматизации тестирования пользовательских интерфейсов.
10. Зачем настраивать строгую политику паролей?

**Вопросы по проверке безопасности кода и управлению уязвимостями**

1. Цели процесса выявления уязвимостей.
2. Какова роль автоматизированных инструментов сканирования кода?
3. Подходы к обнаружению уязвимых зависимостей.
4. Как организовать регулярное тестирование безопасности приложений?
5. Чем полезны динамические тесты (Dynamic Application Security Testing, DAST)?
6. Что входит в процесс Patch Management?
7. Чем Static Analysis Security Testing (SAST) отличается от Dynamic Analysis?
8. Чем является уязвимость нулевого дня (Zero-day vulnerability)?
9. В чём отличие периодической оценки рисков от постоянного мониторинга?
10. Какие стандарты применяют для классификации уязвимостей?

**Вопросы по противодействию DoS/DDoS-атакам**

1. Суть DoS-атаки и её отличия от DDoS.
2. Признаки обнаружения DoS/DDoS-атаки.
3. Эффективные стратегии борьбы с DDoS-атаками.
4. Полезность распределения нагрузки (Load Balancing).
5. Почему важен мониторинг производительности веб-ресурса?
6. Влияние объема входящего трафика на производительность сервера.
7. Практическое применение CDN-сервисов против DDoS.
8. Способны ли аппаратные фаерволлы противостоять современным DDoS-атакам?
9. Что даёт повышение отказоустойчивости инфраструктуры?
10. Стоит ли применять captcha при подозрительных действиях пользователей?

**Вопросы по противодействию XSS-атакам**

1. Разновидности XSS-атак.
2. Пример реализации stored-XSS.
3. Чем опасно внедрение JavaScript-вредоносного кода на странице?
4. Основные подходы к предотвращению XSS.
5. Важно ли использовать экранирование символов?
6. Помогут ли фильтры WAF (Web Application Firewall) от XSS?
7. Насколько эффективны контентные правила CSP?
8. Проблемы безопасности при выполнении асинхронных AJAX-запросов.
9. Есть ли связь между использованием устаревших технологий и риском XSS?
10. Нужно ли проверять данные на выходе в дополнение к данным на входе?

**Вопросы по противодействию атакам внедрения (Injection)**

1. Типичные примеры SQL-инъекций.
2. Возможность обхода фильтров введённых данных.
3. Основной способ предотвращения инъекции кода.
4. Является ли параметризованный SQL-запрос надежным методом защиты?
5. Причины появления PHP-инъекций.
6. Чем грозит OS Command Injection?
7. Безопасность директорий и файлов в Linux относительно инъекционных атак.
8. Зачем проводится проверка путей файлов (Path Validation)?
9. Правила разработки защищенных шаблонов страниц.
10. Достаточно ли одной проверки входящих данных для полной защиты?
11. Основные технологии шифрования данных.

**Вопросы по защите данных и объектов**

1. Важность разделения зон ответственности администратора и разработчика.
2. Ключевые моменты в управлении доступом к ресурсам.
3. Механизмы контроля целостности данных.
4. Чем полезно резервирование и восстановление данных?
5. Почему важны контроль версий и управление изменениями (Change Management)?
6. Кто должен иметь права администрирования баз данных?
7. Недостаточность одних лишь мер по защите базы данных.
8. Средства мониторинга активности сотрудников.
9. Основы многоуровневой защиты данных.
10. Почему небезопасно хранить важные данные в локальном хранилище браузера?

**Вопросы по защите от атак на стороне клиента и сервера**

1. Проблема утечки данных через JavaScript-файлы сторонних разработчиков.
2. Способы снижения риска утечек персональных данных через Google Analytics.
3. Чем опасны атаки click-jacking и как от них защититься?
4. Нужна ли защита от повторного использования сессии (Session Replay)?
5. Критичность использования предсказуемых временных меток для имен файлов.
6. Последствия отсутствия ограниченного числа неудачных попыток входа.
7. Недостаточная защита при обработке загрузочных файлов.
8. Важность фильтрации заголовков запросов.
9. Защищённость путём отключения ненужных служб и модулей на сервере.

**Контрольная работа №1**

**Тема:** Работа с DOM браузера. Построение простого REST API на стороне сервера

**Вопросы:**

1. Что такое объектная модель документа (DOM)? Какова её роль в веб-разработке?
2. Опишите основные методы и свойства объекта `document` в JavaScript.
3. Какие события используются для отслеживания изменений в DOM? Приведите пример реализации обработчика события изменения элемента страницы.
4. Объясните принцип построения RESTful API. Назовите преимущества такого подхода перед SOAP.
5. Напишите простой сервер на Node.js, реализующий метод GET для получения списка пользователей из базы данных.
6. Чем отличается асинхронная обработка запросов от синхронной? Приведите пример обоих подходов в коде.
7. Опишите процесс взаимодействия клиентской части приложения с сервером через AJAX-запросы. Покажите реализацию отправки POST-запроса.
8. Какие существуют форматы передачи данных в REST API? Укажите наиболее распространённые и опишите их особенности.
9. Почему важно правильно обрабатывать запросы и ошибки в REST API? Какие подходы применяются для возврата ошибок клиенту?
10. Какие средства защиты рекомендуется применять при разработке REST API?

**Контрольная работа №2**

**Тема:** Анализ атак на стороне клиента. Анализ атак на стороне сервера

**Вопросы:**

1. Перечислите и поясните основные виды атак на стороне клиента. Дайте определение каждой атаки.
2. Описать механизм межсайтового скриптинга (XSS). Привести практические рекомендации по защите от него.
3. Что такое CSRF? Какой способ защиты от подделки межсайтовых запросов является наиболее эффективным?
4. Как злоумышленники используют уязвимости SQL Injection? Предложите меры противодействия этому виду атак.
5. Опишите типичные способы обхода аутентификации и авторизации на стороне сервера. Какие механизмы защиты позволяют минимизировать риск взлома учётных записей?
6. В чём заключается атака типа Man-in-the-Middle (MITM)? Какие инструменты могут использоваться для защиты от неё?
7. Какие проблемы возникают при обработке файлов загружаемых пользователями на сервер? Как предотвратить эксплуатацию этих проблем?
8. Расскажите о механизмах обнаружения вторжений IDS и IPS. Для чего предназначены эти системы?
9. Чем отличаются атаки Brute Force и Dictionary Attacks? Какие меры защиты эффективны против этих методов подбора паролей?
10. Что такое Buffer Overflow? Как защититься от подобных атак на уровне разработки программного обеспечения?

**Контрольная работа №3**

**Тема:** Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности

**Вопросы:**

1. Дайте определения следующим терминам: угроза, риск, уязвимость. Как связаны эти понятия друг с другом?

2. Охарактеризуйте типы угроз информационной безопасности: внутренние и внешние угрозы. Приведите примеры каждой группы.
3. Изобразите классификацию рисков информационной безопасности согласно ISO 27001. Опишите значение каждого уровня риска.
4. Что представляет собой киберугроза APT (Advanced Persistent Threat)? Чем она опасна и какие методы борьбы рекомендуются?
5. Что такое аудит информационной безопасности? Каковы цели и этапы проведения аудита?
6. Определите понятие DDoS-атаки. По каким признакам можно определить такую атаку? Какие защитные механизмы помогают смягчить последствия нападения?
7. Перечислите известные международные стандарты в области информационной безопасности. Кратко охарактеризуйте каждый стандарт.
8. Объясните разницу между антивирусом и файрволлом. Когда используется одно средство защиты, а когда другое?
9. Что такое двухфакторная аутентификация (2FA)? Зачем она применяется и какие технологии используются для её реализации?
10. Опишите базовые принципы управления доступом RBAC (Role-Based Access Control).

**Контрольная работа №4**

**Тема:** Работа с протоколами HTTP, HTTPS. Анализ входящего/исходящего трафика. Использование сетевых утилит

**Вопросы:**

1. Чем отличается протокол HTTP от протокола HTTPS? Как устроено шифрование данных в HTTPS?
2. Опишите структуру HTTP-запроса и HTTP-ответа. Перечислите основные заголовки и их назначение.
3. Какие состояния соединения возможны в HTTP-протоколе? Опишите сценарии использования разных состояний.
4. Приведите описание формата JSON и XML. В каких случаях предпочтительнее использовать тот или иной формат?
5. Как анализировать исходящие и входящие пакеты сети с использованием Wireshark? Какие возможности анализа предоставляет эта программа?
6. Опишите инструмент netstat. Какая полезная информация может быть извлечена с его помощью?
7. Какие команды Unix-подобных операционных систем используются для диагностики сетей и мониторинга соединений?
8. Назначение инструмента curl. Продемонстрируйте синтаксис команд для проверки доступности сайта, загрузки файла и отправку POST-запросов.
9. Какие стандартные порты используются HTTP и HTTPS? Есть ли разница в назначении этих протоколов относительно используемых ими портов?
10. Рассмотрите различия между TCP и UDP-протоколами. Какие ситуации требуют выбора именно TCP, а какие — UDP?

**Контрольная работа №5**

**Тема:** Разработка безопасной конфигурации приложений. Обеспечение безопасности пользовательского интерфейса

**Вопросы:**

1. Что означает термин "безопасная конфигурация"? Как настраивать приложение таким образом, чтобы минимизировать возможные угрозы?
2. Что такое cookie и сессии? Какие опасности возникают при некорректной работе с ними? Приведите правила настройки cookie и сессий.

3. Опишите принципы защиты от Cross-Site Request Forgery (CSRF). Какие методы предотвращения чаще всего используются разработчиками?
4. Назовите лучшие практики обеспечения безопасности пользовательских интерфейсов. Как проверить наличие защищённых элементов в приложении?
5. Какие механизмы аутентификации и авторизации применяют современные web-приложения? Проанализируйте плюсы и минусы популярных решений.
6. Что такое HSTS (HTTP Strict Transport Security)? Как его использование повышает безопасность сайта?
7. Что включает в себя защита инфраструктуры приложений? Перечислите обязательные элементы защиты инфраструктуры.
8. Приведите основные техники ограничения привилегий и минимизации прав пользователей.
9. Что значит понятие "Least Privilege Principle"? Где оно применимо и почему важно соблюдать этот принцип?
10. Какие методы защиты от внедрения вредоносного ПО используются в современных приложениях?

**Контрольная работа №6**

**Тема:** Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями

**Вопросы:**

1. Перечислите и объясните основные методы тестирования безопасности приложений (белый ящик, чёрный ящик, серый ящик).
2. Что такое статический анализ кода? Какие инструменты используют разработчики для выявления потенциальных уязвимостей?
3. Какие существуют динамические методы тестирования безопасности? Какие недостатки и преимущества у этих методов?
4. Что такое Penetration Testing (pen testing)? В чём отличие внешнего pen-тестирования от внутреннего?
5. Что такое OWASP Top Ten? Какие уязвимости входят в список наиболее опасных угроз безопасности веб-приложений?
6. Как осуществляется управление уязвимостями в организации? Какие процессы включаются в жизненный цикл обработки уязвимостей?
7. Какие методики оценки степени критичности выявленных уязвимостей вам известны?
8. В чём состоит методика Risk Assessment и почему она важна при оценке уязвимостей?
9. Почему возникает необходимость постоянного обновления и патчинга программного обеспечения? Какие шаги предпринимает организация для своевременного устранения найденных уязвимостей?
10. В чём заключается процедура Incident Response Plan (IRP)? Почему такая политика необходима организациям?

**Контрольная работа №7**

**Тема:** Противодействие DoS-атакам. Противодействие XSS-атакам. Противодействие внедрению

**Вопросы:**

1. Что такое Denial of Service (DoS)-атака? Как различается DoS и Distributed Denial of Service (DDoS)?
2. Опишите технологию Content Delivery Network (CDN) и как она помогает защитить сайт от DDoS-атак.
3. В чём опасность XSS-внедрения? Какие формы существования кросс-сайтовых скриптов существуют?

4. Приведите примеры мер защиты от XSS-уязвимостей. Какие дополнительные инструменты защиты могут усилить защиту сайта?
5. Что такое внедрение произвольного кода (Code Injection)? Приведите конкретные примеры и предложите эффективные контрмеры.
6. Почему важно фильтровать вводимую пользователем информацию на сервере? Какие функции встроены в PHP, Python и Ruby для очистки данных?
7. Чем опасно File Upload злоупотребление? Какие правила и советы следует учитывать при проектировании механизмов загрузки файлов?
8. Приведите алгоритм детектирования аномалий сетевого трафика при подозрении на проведение DDoS-атаки.
9. Что такое HTTP flood attack? Какими средствами бороться с такими видами атак?
10. Какие решения предлагаются для защиты корпоративной инфраструктуры от проникновения через SSL-туннели?

**Контрольная работа №8**

**Тема:** Защита данных и объектов. Защита от атак на стороне клиента. Защита от атак на стороне сервера

**Вопросы:**

1. В чём суть принципов целостности, конфиденциальности и доступности данных? Приведите пример нарушения каждого принципа.
2. Что такое хранение данных "на стороне клиента"? Какие угрозы и меры защиты связаны с данным способом хранения?
3. Перечислите уровни доступа к данным в корпоративных системах. Какие роли и права ассоциируются с каждым уровнем?
4. Что понимается под защитой информации "in transit" ("в пути")? Какие методы криптографии применяются для обеспечения защиты передаваемой информации?
5. Приведите три основных метода защиты баз данных от несанкционированного доступа. Опишите, как они работают.
6. Как организовать политику резервного копирования и восстановления данных? Какие критерии определяют частоту и глубину резервного копирования?
7. В чём состоят отличия локальных хранилищ (LocalStorage, SessionStorage) от cookies? Какие преимущества и недостатки имеет каждое решение?
8. Опишите стратегию защиты конфиденциальных данных путём разделения ответственности и ролей. Какие специалисты участвуют в обеспечении безопасности данных?
9. Какие общие стратегии защиты баз данных вы знаете? Как обеспечить целостность и доступность хранимых данных?
10. Что такое data masking и зачем он нужен? Приведите примеры использования маскировки данных в реальных проектах.

Направление подготовки: 09.00.00 Информатика и вычислительная техника

(шифр и наименование направления подготовки/специальности)

Профиль: 09.03.01 Автоматизированные системы обработки информации и управление

(наименование профиля)

Дисциплина: Б1.В.ДВ.01.06 Обеспечение безопасности web-приложений

(шифр и наименование дисциплины в соответствии с учебным планом)

| Номер задания | Содержание задания | Ключ к ответу | Наименование темы РПД | Семестр |
|---|---|---|---|---|
| **ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению** | | | | |
| 1. | Прочитайте текст вопроса и выберите правильный ответ:<br>Укажите основную цель кибербезопасности.<br>1. Максимизация скорости работы системы<br>2. Увеличение объёма хранимых данных<br>3. Обеспечение конфиденциальности, целостности и доступности информации<br>4. Снижение стоимости оборудования | 3 | Информационная безопасность: основные понятия | 5 |
| 2. | Прочитайте текст вопроса и выберите правильный ответ:<br>Укажите, что относится к основным угрозам в сфере кибербезопасности.<br>1. Повышение производительности оборудования<br>2. Несанкционированный доступ, вредоносное ПО и DDoS-атаки<br>3. Обновление программного обеспечения<br>4. Увеличение количества пользователей | 2 | Анализ угроз Web-приложениям | 5 |
| 3. | Прочитайте текст вопроса и выберите два правильных ответа:<br>Укажите виды шифрования, которые применяются в кибербезопасности.<br>1. Симметричное шифрование<br>2. Стеганография<br>3. Асимметричное шифрование<br>4. Хеширование без ключа | 13 | Методы защиты Web-приложений | 5 |
| 4. | Прочитайте текст вопроса и выберите два правильных ответа:<br>Укажите основные угрозы в сфере кибербезопасности.<br>1. Обновление антивирусных баз<br>2. Фишинг<br>3. Регулярное резервное копирование<br>4. DDoS-атака<br>5. Установка лицензионного ПО | 24 | Анализ угроз Web-приложениям | 5 |
| 5. | Прочитайте текст вопроса и установите последовательность.<br>Запишите соответствующую последовательность цифр слева направо.<br>Установите правильную последовательность этапов создания электронной цифровой подписи.<br>1. Проверка подлинности ЭП получателем<br>2. Вычисление хеш-функции от документа<br>3. Передача документа получателю<br>4. Шифрование хеша закрытым ключом отправителя | 2431 | 4 | 5. |
| 5. | Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность букв слева направо.<br>Установите последовательность этапов алгоритма tls handshake<br>1. Аутентификация и обмен ключами<br>2. Ответ сервера | 42135 | Методы защиты Web-приложений | 5 |

| | | | | |
|---|---|---|---|---|
| | 3. Завершение рукопожатия<br>4. Инициация соединения<br>5. Защищенный обмен данными | | | |
| ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию | | | | |
| 6. | Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность букв слева направо.<br>Установите последовательность действий при использовании шифра XOR.<br>1. Преобразовать ключ в двоичный код<br>2. Преобразовать исходное сообщение в двоичный код<br>3. Выбрать ключ (символ или набор символов, который участвует в операции XOR с каждым байтом или символом входных данных открытого текста)<br>4. Применить операцию XOR | 3124 | Методы защиты Web-приложений | 5 |
| 7. | Прочитайте текст и установите соответствие.<br>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца.<br>Запишите выбранные цифры под соответствующими буквами.<br>Вид атаки<br>A. Brute-force<br>B. Man-in-the-middle<br>C. DDoS<br>D. SQL-инъекция<br><br>1. Внедрение вредоносного кода через формы ввода<br>2. Перехват и подмена трафика между сторонами<br>3. Полный перебор всех возможных комбинаций<br>4. Перегрузка сервера множеством запросов | A-3 B-2 C-4 D-1 | Анализ угроз Web-приложениям | 5 |
| 8. | Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.<br>Метод защиты<br>A) Симметричное шифрование<br>B) Асимметричное шифрование<br>C) Стеганография<br>D) Хеширование<br><br>1) Использование пары ключей (открытый и закрытый)<br>2) Использование одного секретного ключа<br>3) Преобразование данных в короткое значение фиксированной длины<br>4) Скрытие факта наличия информации внутри другого файла | A-2 B-1 C-4 D-3 | Методы защиты Web-приложений | 5 |
| 9. | Прочитайте текст и дополните фразу:<br>В симметричном шифровании один и тот же ключ используется как для _____ , так и для _____. | шифрования / расшифрования | Методы защиты Web-приложений | 5 |
| 10. | Прочитайте текст и дополните фразу:<br>Основной целью пенетрационного тестирования является выявление _____ в системе защиты. | уязвимостей | Методы защиты Web-приложений | 5 |

Направление подготовки: 09.00.00 Информатика и вычислительная техника

(шифр и наименование направления подготовки/специальности)

Профиль: 09.03.01 Автоматизированные системы обработки информации и управление

(наименование профиля)

Дисциплина: Б1.В.ДВ.01.06 Обеспечение безопасности web-приложений

(шифр и наименование дисциплины в соответствии с учебным планом)

| Номер задания | Содержание задания | Ключ к ответу | Наименование темы РПД | Семестр |
|---|---|---|---|---|
| **ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению** | | | | |
| 1. | Прочитайте текст вопроса и выберите правильный ответ:<br>Укажите основную цель кибербезопасности.<br>1. Максимизация скорости работы системы<br>2. Увеличение объёма хранимых данных<br>3. Обеспечение конфиденциальности, целостности и доступности информации<br>4. Снижение стоимости оборудования | 3 | Информационная безопасность: основные понятия | 5 |
| 2. | Прочитайте текст вопроса и выберите правильный ответ:<br>Укажите, что относится к основным угрозам в сфере кибербезопасности.<br>1. Повышение производительности оборудования<br>2. Несанкционированный доступ, вредоносное ПО и DDoS-атаки<br>3. Обновление программного обеспечения<br>4. Увеличение количества пользователей | 2 | Анализ угроз Web-приложениям | 5 |
| 3. | Прочитайте текст вопроса и выберите два правильных ответа:<br>Укажите виды шифрования, которые применяются в кибербезопасности.<br>1. Симметричное шифрование<br>2. Стеганография<br>3. Асимметричное шифрование<br>4. Хеширование без ключа | 13 | Методы защиты Web-приложений | 5 |
| 4. | Прочитайте текст вопроса и выберите два правильных ответа:<br>Укажите основные угрозы в сфере кибербезопасности.<br>1. Обновление антивирусных баз<br>2. Фишинг<br>3. Регулярное резервное копирование<br>4. DDoS-атака<br>5. Установка лицензионного ПО | 24 | Анализ угроз Web-приложениям | 5 |
| 5. | Прочитайте текст вопроса и установите последовательность.<br>Запишите соответствующую последовательность цифр слева направо.<br>Установите правильную последовательность этапов создания электронной цифровой подписи.<br>1. Проверка подлинности ЭП получателем<br>2. Вычисление хеш-функции от документа<br>3. Передача документа получателю<br>4. Шифрование хеша закрытым ключом отправителя | 2431 | 4 | 5. |
| 5. | Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность букв слева направо.<br>Установите последовательность этапов алгоритма tls handshake<br>1. Аутентификация и обмен ключами<br>2. Ответ сервера | 42135 | Методы защиты Web-приложений | 5 |

| | | | | |
|---|---|---|---|---|
| | 3. Завершение рукопожатия<br>4. Инициация соединения<br>5. Защищенный обмен данными | | | |
| ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию | | | | |
| 6. | Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность букв слева направо.<br>Установите последовательность действий при использовании шифра XOR.<br>1. Преобразовать ключ в двоичный код<br>2. Преобразовать исходное сообщение в двоичный код<br>3. Выбрать ключ (символ или набор символов, который участвует в операции XOR с каждым байтом или символом входных данных открытого текста)<br>4. Применить операцию XOR | 3124 | Методы защиты Web-приложений | 5 |
| 7. | Прочитайте текст и установите соответствие.<br>К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца.<br>Запишите выбранные цифры под соответствующими буквами.<br>Вид атаки<br>A. Brute-force<br>B. Man-in-the-middle<br>C. DDoS<br>D. SQL-инъекция<br><br>1. Внедрение вредоносного кода через формы ввода<br>2. Перехват и подмена трафика между сторонами<br>3. Полный перебор всех возможных комбинаций<br>4. Перегрузка сервера множеством запросов | A-3 B-2 C-4 D-1 | Анализ угроз Web-приложениям | 5 |
| 8. | Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.<br>Метод защиты<br>A) Симметричное шифрование<br>B) Асимметричное шифрование<br>C) Стеганография<br>D) Хеширование<br><br>1) Использование пары ключей (открытый и закрытый)<br>2) Использование одного секретного ключа<br>3) Преобразование данных в короткое значение фиксированной длины<br>4) Скрытие факта наличия информации внутри другого файла | A-2 B-1 C-4 D-3 | Методы защиты Web-приложений | 5 |
| 9. | Прочитайте текст и дополните фразу:<br>В симметричном шифровании один и тот же ключ используется как для _____ , так и для _____. | шифрования / расшифрования | Методы защиты Web-приложений | 5 |
| 10. | Прочитайте текст и дополните фразу:<br>Основной целью пенетрационного тестирования является выявление _____ в системе защиты. | уязвимостей | Методы защиты Web-приложений | 5 |