Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ **ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ**

КАФЕДРА **КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.03.01 Информатика и вычислительная техника**

О Т Ч Е Т

по домашней работе № 1

Дисциплина: Защита информации

Студент	ИУ6-82Б		С.В. Астахов
	(Группа)	(Подпись, дата)	(И.О. Фамилия)
Преподаватель			Д.А. Миков
		(Подпись, дата)	(И.О. Фамилия)

Москва, 2023

Цель: Выявить риски нарушения целостности, доступности и/или конфиденциальности в заданной автоматизированной системе и разработать для нее политику безопасности.

Исследовать информационные процессы в заданной автоматизированной системе и предложить средства и методы для их защиты.

Объект защиты: Подсистема тестирования знаний для образовательного портала (тема ВКРБ).

Термины и определения

Нарушение целостности информации — повреждение или непредвиденное изменение данных, значительно увеличивающее опасность их использования. Помимо вероятности потерять важные сведения, в тяжелых случаях существует риск утраты работоспособности всей системы в целом.

Нарушение доступности информации — создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

Нарушение конфиденциальности — утечка данных, несанкционированный доступ или разглашение информации.

Характеристика рассматриваемой системы

Рассматриваемая подсистема является подсистемой тестирования знаний для образовательного портала. Система позволяет хранить информацию, проверять решения и сохранять историю решений для тестовых заданий и заданий на программирование.

Входные данные:

- информация о сущностях предметной области (пользователи, задания и т.д.) в формате JSON;
- исходный код на языке Verilog;
- описание тестовых заданий в специальном внутреннем формате.

Выходные данные:

- информация о сущностях предметной области (пользователи, задания и т.д.) в формате JSON;

- информация о пользовательской статистике и ошибках в заданиях в формате JSON.

Основные информационные процессы в заданной системе:

- создание, изменение, удаление информации о задании в БД администратором;

- чтение информации о задания из БД;

- чтение статистики прохождения заданий;

- проверка правильности задания (может включать работу с исходным кодом на языке Verilog).

Выявление угроз

Рассмотрим возможные угрозы и методы защиты от них с помощью концептуальной модели безопасности (рисунок 1).

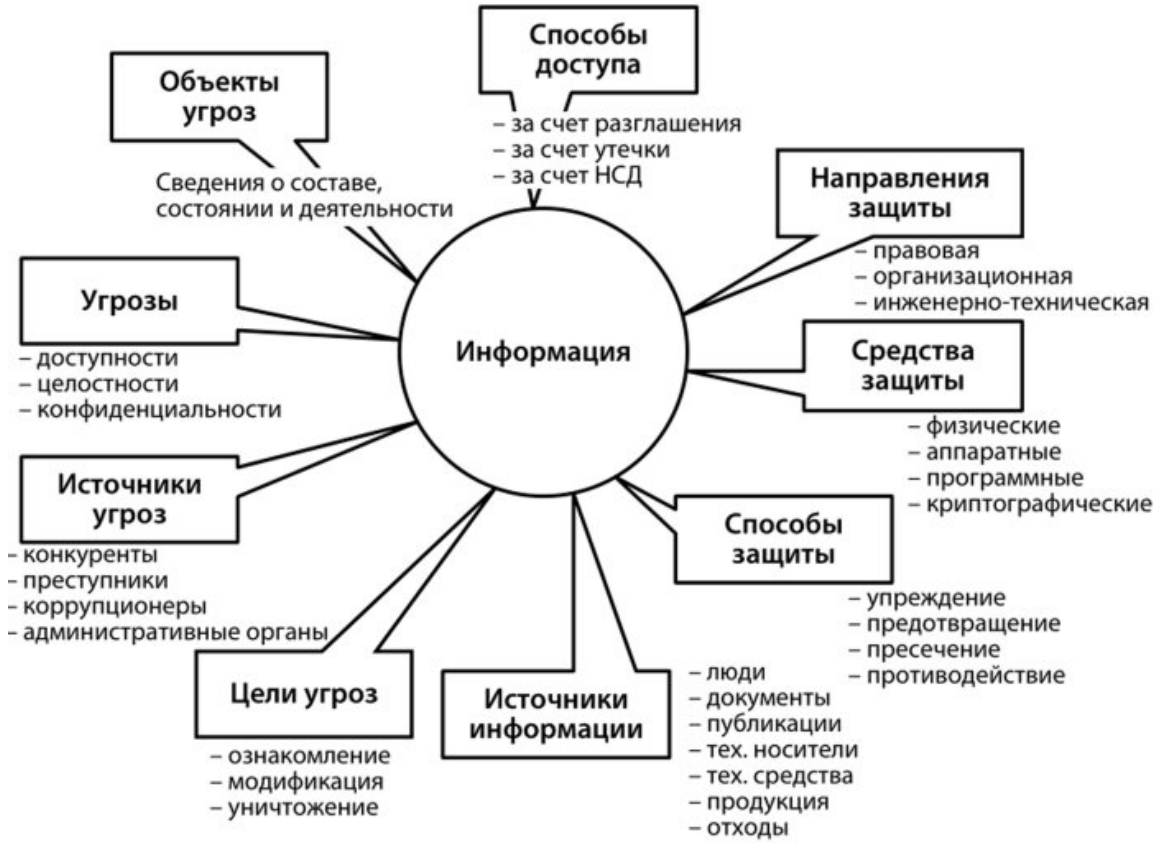

Рисунок 1 — концептуальная модель безопасности

В рассматриваемом случае:

Объект угрозы: Подсистема тестирования знаний для образовательного портала (тема ВКРБ).

Направление защиты: инженерно-техническое.

Средства защиты: программные.

Способы защиты: упреждение.

Опираясь на характеристику системы и концептуальную модель безопасности, попытаемся выявить угрозы и методы противодействия им (таблица 1).

Таблица 1 — угрозы и методы противодействия

Угроза	Вид угрозы	Способ устранения
Доступ к подсистеме с постороннего IP-адреса (не из основной системы)	Конфиденциальности	1. Настройка сети таким образом, чтобы доступ к подсистеме из «внешнего мира» был невозможен на уровне сети 2. Использование механизма авторизации между основной системой и подсистемой (например, JWT-токенов)

Продолжение таблицы 1

SQL-инъекции в запросах к БД	Целостности	Экранирование параметров запроса при обращении к БД
Нарушение формата при создании/изменении информации о тестовых заданиях	Целостности	Проверка корректности формата описания тестовых заданий перед внесением изменений
Нарушение целостности информации БД вследствие аппаратного сбоя	Целостности	Создание резервных копий
Недоступности подсистемы из-за слишком высокой нагрузки	Доступности	Балансировка нагрузки, использование master-slave репликации БД

Вывод: были выявлены риски нарушения целостности, конфиденциальности и доступности в заданной автоматизированной системе и разработана для нее политика безопасности.