РНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий (ИКБ)

КБ-2 «Информационно-аналитические системы кибербезопасности»

ОТЧЕТ О ВЫПОЛНЕНИИ ЗАДАНИЯ №4

В РАМКАХ ДИСЦИПЛИНЫ «МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ»

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

Оглавление

Задание

Объект защиты: сервер базы данных компании.

Цель: Идентификация и классификация актуальных угроз безопасности информации, потенциально воздействующих на сервер базы данных компании, с учётом нарушителей и возможных последствий согласно ГОСТу 51275-2006.

№ УБИ	Название УБИ	Описание	Нарушитель и его уровень возможностей	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
1	Несанкционированный доступ к данным БД	Получение пользователем или процессом доступа к данным, не разрешенным политикой безопасности.	Внутренний/внешний нарушитель, средний уровень	Да	Нет	Нет
2	Несанкционированная модификация данных	Изменение, удаление или подмена данных в базе данных без соответствующих полномочий.	Внутренний нарушитель, высокий уровень	Нет	Да	Нет
3	Отказ в обслуживании (DoS/DDoS)	Создание условий, при которых легитимные пользователи лишаются доступа к серверу БД из-за исчерпания ресурсов.	Внешний нарушитель, высокий уровень	Нет	Нет	Да
4	Несанкционированный доступ к конфигурации СУБД	Изменение параметров конфигурации сервера БД, ведущее к снижению уровня безопасности.	Внутренний нарушитель, высокий уровень	Да	Да	Да
5	Внедрение вредоносного кода (SQL-инъекция)	Внедрение и выполнение произвольного SQL-кода через уязвимости в клиентских приложениях.	Внешний нарушитель, средний уровень	Да	Да	Нет
6	Компрометация учетных данных	Хищение или подбор учетных данных (логинов/паролей) легитимных пользователей или администраторов БД.	Внутренний/внешний нарушитель,	Да	Да	Да

			средний уровень			
7	Неправомерное изменение схемы БД	Несанкционированное создание, изменение или удаление объектов базы данных (таблиц, представлений, процедур).	Внутренний нарушитель, высокий уровень	Нет	Да	Нет
8	Утечка информации через побочные каналы	Несанкционированное получение информации за счет анализа побочных эффектов работы системы (время отклика, электромагнитное излучение).	Внешний нарушитель, высокий уровень	Да	Нет	Нет
9	Нарушение регламента резервного копирования	Сбой или намеренное нарушение процесса резервного копирования, ведущее к невозможности восстановления данных.	Внутренний нарушитель, низкий уровень	Нет	Нет	Да
10	Несанкционированный доступ к файлам резервных копий	Хищение или копирование файлов резервных копий базы данных.	Внутренний нарушитель, средний уровень	Да	Нет	Нет
11	Отказ аппаратного обеспечения	Выход из строя оборудования сервера (дисковый массив, память, процессор), ведущий к недоступности БД.	Техногенный фактор (не нарушитель)	Нет	Нет	Да
12	Несанкционированное использование привилегий	Использование легальных высоких привилегий для совершения несанкционированных действий (например, администратором).	Внутренний нарушитель, высокий уровень	Да	Да	Нет
13	Перехват данных в канале связи	Несанкционированный перехват информации, передаваемой между клиентским приложением и сервером БД.	Внешний нарушитель, средний уровень	Да	Нет	Нет
14	Нарушение целостности транзакций	Намеренное или случайное нарушение логики транзакций, приводящее к несогласованности данных.	Внутренний нарушитель, средний уровень	Нет	Да	Нет
15	Несанкционированный доступ к журналам аудита	Получение доступа к журналам регистрации событий безопасности для сокрытия других атак.	Внутренний нарушитель,	Да	Нет	Нет

			средний уровень			
16	Неправомерное восстановление данных	Восстановление данных из резервной копии в обход установленных процедур, что может привести к потере актуальных данных.	Внутренний нарушитель, средний уровень	Нет	Да	Нет
17	Внедрение вредоносного ПО на уровне ОС	Установка на сервер БД вредоносных программ (трояны, шпионское ПО), нарушающих политику безопасности.	Внешний нарушитель, высокий уровень	Да	Да	Да
18	Несанкционированное создание учетных записей	Создание в СУБД новых учетных записей с правами доступа к данным.	Внутренний нарушитель, высокий уровень	Да	Да	Нет
19	Нарушение физической безопасности сервера	Прямой физический доступ к оборудованию сервера БД, позволяющий изменить его конфигурацию или похитить диски.	Внутренний нарушитель, низкий уровень	Да	Да	Да
20	Неправомерное блокирование данных	Намеренная установка блокировок на данные или объекты БД, препятствующая работе легитимных пользователей.	Внутренний нарушитель, средний уровень	Нет	Нет	Да
21	Несанкционированное использование служебных утилит	Использование административных утилит СУБД или ОС для обхода механизмов защиты и несанкционированного доступа к данным.	Внутренний нарушитель, высокий уровень	Да	Да	Нет
22	Недостатки в системе управления доступом	Ошибки в настройке или проектировании системы разграничения прав доступа, позволяющие нарушителю получить несанкционированные привилегии.	Внутренний нарушитель, средний уровень	Да	Да	Нет
23	Нарушение регламента обслуживания	Несоблюдение установленных процедур и регламентов по обслуживанию БД (например, установка патчей), ведущее к появлению уязвимостей.	Внутренний нарушитель, низкий уровень	Нет	Да	Да
24	Несанкционированное подключение к	Доступ к интерфейсам удаленного администрирования СУБД или ОС сервера БД.	Внешний нарушитель,	Да	Да	Да

	административным интерфейсам		высокий уровень			
25	Потеря или хищение носителей информации	Утрата или кража физических носителей (жестких дисков, лент), на которых хранится база данных или ее резервные копии.	Внутренний/внешний нарушитель, низкий уровень	Да	Нет	Нет

Таблица 1 - Модель угроз

Метод непосредственной оценки

Сопроводительный текст для таблиц.

«Уважаемый эксперт, для работы Вам представлен набор угроз ИБ сервера базы данных предприятия ООО «Финмониторинг», функционирующего в сфере оказания финансовых услуг и автоматизации бухгалтерского учета. Просим Вас оценить возможность реализации каждой из обозначенных угроз ИБ на информационно-аналитическую систему предприятия и отразить свое мнение в таблице:

№ УБИ	Название УБИ	Описание	Оценка (1-10)
1			

Шкала для оценивания [0,10], где

10 баллов - критическая угроза (высокая вероятность реализации, катастрофические последствия)

7-9 баллов - высокая угроза (вероятность реализации выше среднего, серьезные последствия)

4-6 баллов - средняя угроза (умеренная вероятность, ощутимые последствия)

1-3 балла - низкая угроза (маловероятная реализация, незначительные последствия)»

Заполненные экспертами таблицы представлены далее.

№ УБИ	Название УБИ	Описание	Оценка (1-10)
1	Несанкционированный доступ к данным БД	Получение пользователем или процессом доступа к данным, не разрешенным политикой безопасности.	9
2	Несанкционированная модификация данных	Изменение, удаление или подмена данных в базе данных без соответствующих полномочий.	8
3	Отказ в обслуживании (DoS/DDoS)	Создание условий, при которых легитимные пользователи лишаются доступа к серверу БД из-за исчерпания ресурсов.	7
4	Несанкционированный доступ к конфигурации СУБД	Изменение параметров конфигурации сервера БД, ведущее к снижению уровня безопасности.	8
5	Внедрение вредоносного кода (SQL-инъекция)	Внедрение и выполнение произвольного SQL-кода через уязвимости в клиентских приложениях.	9
6	Компрометация учетных данных	Хищение или подбор учетных данных (логинов/паролей) легитимных пользователей или администраторов БД.	9
7	Неправомерное изменение схемы БД	Несанкционированное создание, изменение или удаление объектов базы данных (таблиц, представлений, процедур).	7
8	Утечка информации через побочные каналы	Несанкционированное получение информации за счет анализа побочных эффектов работы системы (время отклика, электромагнитное излучение).	6
9	Нарушение регламента резервного копирования	Сбой или намеренное нарушение процесса резервного копирования, ведущее к невозможности восстановления данных.	5
10	Несанкционированный доступ к файлам резервных копий	Хищение или копирование файлов резервных копий базы данных.	8
11	Отказ аппаратного обеспечения	Выход из строя оборудования сервера (дисковый массив, память, процессор), ведущий к недоступности БД.	4
12	Несанкционированное использование привилегий	Использование легальных высоких привилегий для совершения несанкционированных действий (например, администратором).	8
13	Перехват данных в канале связи	Несанкционированный перехват информации, передаваемой между клиентским приложением и сервером БД.	7
14	Нарушение целостности транзакций	Намеренное или случайное нарушение логики транзакций, приводящее к несогласованности данных.	6
15	Несанкционированный доступ к журналам аудита	Получение доступа к журналам регистрации событий безопасности для сокрытия других атак.	5
16	Неправомерное восстановление данных	Восстановление данных из резервной копии в обход установленных процедур, что может привести к потере актуальных данных.	6

17	Внедрение вредоносного ПО на уровне ОС	Установка на сервер БД вредоносных программ (трояны, шпионское ПО), нарушающих политику безопасности.	8
18	Несанкционированное создание учетных записей	Создание в СУБД новых учетных записей с правами доступа к данным.	7
19	Нарушение физической безопасности сервера	Прямой физический доступ к оборудованию сервера БД, позволяющий изменить его конфигурацию или похитить диски.	9
20	Неправомерное блокирование данных	Намеренная установка блокировок на данные или объекты БД, препятствующая работе легитимных пользователей.	5
21	Несанкционированное использование служебных утилит	Использование административных утилит СУБД или ОС для обхода механизмов защиты и несанкционированного доступа к данным.	7
22	Недостатки в системе управления доступом	Ошибки в настройке или проектировании системы разграничения прав доступа, позволяющие нарушителю получить несанкционированные привилегии.	6
23	Нарушение регламента обслуживания	Несоблюдение установленных процедур и регламентов по обслуживанию БД (например, установка патчей), ведущее к появлению уязвимостей.	5
24	Несанкционированное подключение к административным интерфейсам	Доступ к интерфейсам удаленного администрирования СУБД или ОС сервера БД.	8
25	Потеря или хищение носителей информации	Утрата или кража физических носителей (жестких дисков, лент), на которых хранится база данных или ее резервные копии.	7

Таблица 2 - Оценки эксперта 1, при методе непосредственной оценки

№ УБИ	Название УБИ	Описание	Оценка (1-10)
1	Несанкционированный доступ к данным БД	Получение пользователем или процессом доступа к данным, не разрешенным политикой безопасности.	8
2	Несанкционированная модификация данных	Изменение, удаление или подмена данных в базе данных без соответствующих полномочий.	9
3	Отказ в обслуживании (DoS/DDoS)	Создание условий, при которых легитимные пользователи лишаются доступа к серверу БД из-за исчерпания ресурсов.	9
4	Несанкционированный доступ к конфигурации СУБД	Изменение параметров конфигурации сервера БД, ведущее к снижению уровня безопасности.	7
5	Внедрение вредоносного кода (SQL-инъекция)	Внедрение и выполнение произвольного SQL-кода через уязвимости в клиентских приложениях.	8
6	Компрометация учетных данных	Хищение или подбор учетных данных (логинов/паролей) легитимных пользователей или администраторов БД.	8
7	Неправомерное изменение схемы БД	Несанкционированное создание, изменение или удаление объектов базы данных (таблиц, представлений, процедур).	8
8	Утечка информации через побочные каналы	Несанкционированное получение информации за счет анализа побочных эффектов работы системы (время отклика, электромагнитное излучение).	5
9	Нарушение регламента резервного копирования	Сбой или намеренное нарушение процесса резервного копирования, ведущее к невозможности восстановления данных.	8
10	Несанкционированный доступ к файлам резервных копий	Хищение или копирование файлов резервных копий базы данных.	7
11	Отказ аппаратного обеспечения	Выход из строя оборудования сервера (дисковый массив, память, процессор), ведущий к недоступности БД.	7
12	Несанкционированное использование привилегий	Использование легальных высоких привилегий для совершения несанкционированных действий (например, администратором).	8
13	Перехват данных в канале связи	Несанкционированный перехват информации, передаваемой между клиентским приложением и сервером БД.	6
14	Нарушение целостности транзакций	Намеренное или случайное нарушение логики транзакций, приводящее к несогласованности данных.	7
15	Несанкционированный доступ к журналам аудита	Получение доступа к журналам регистрации событий безопасности для сокрытия других атак.	6
16	Неправомерное восстановление данных	Восстановление данных из резервной копии в обход установленных процедур, что может привести к потере актуальных данных.	6

17	Внедрение вредоносного ПО на уровне ОС	Установка на сервер БД вредоносных программ (трояны, шпионское ПО), нарушающих политику безопасности.	8
18	Несанкционированное создание учетных записей	Создание в СУБД новых учетных записей с правами доступа к данным.	7
19	Нарушение физической безопасности сервера	Прямой физический доступ к оборудованию сервера БД, позволяющий изменить его конфигурацию или похитить диски.	8
20	Неправомерное блокирование данных	Намеренная установка блокировок на данные или объекты БД, препятствующая работе легитимных пользователей.	6
21	Несанкционированное использование служебных утилит	Использование административных утилит СУБД или ОС для обхода механизмов защиты и несанкционированного доступа к данным.	7
22	Недостатки в системе управления доступом	Ошибки в настройке или проектировании системы разграничения прав доступа, позволяющие нарушителю получить несанкционированные привилегии.	7
23	Нарушение регламента обслуживания	Несоблюдение установленных процедур и регламентов по обслуживанию БД (например, установка патчей), ведущее к появлению уязвимостей.	6
24	Несанкционированное подключение к административным интерфейсам	Доступ к интерфейсам удаленного администрирования СУБД или ОС сервера БД.	8
25	Потеря или хищение носителей информации	Утрата или кража физических носителей (жестких дисков, лент), на которых хранится база данных или ее резервные копии.	6

Таблица 3 - Оценки эксперта 2, при методе непосредственной оценки

№ УБИ	Название УБИ	Описание	Оценка (1-10)
1	Несанкционированный доступ к данным БД	Получение пользователем или процессом доступа к данным, не разрешенным политикой безопасности.	7
2	Несанкционированная модификация данных	Изменение, удаление или подмена данных в базе данных без соответствующих полномочий.	8
3	Отказ в обслуживании (DoS/DDoS)	Создание условий, при которых легитимные пользователи лишаются доступа к серверу БД из-за исчерпания ресурсов.	8
4	Несанкционированный доступ к конфигурации СУБД	Изменение параметров конфигурации сервера БД, ведущее к снижению уровня безопасности.	7
5	Внедрение вредоносного кода (SQL-инъекция)	Внедрение и выполнение произвольного SQL-кода через уязвимости в клиентских приложениях.	9
6	Компрометация учетных данных	Хищение или подбор учетных данных (логинов/паролей) легитимных пользователей или администраторов БД.	8
7	Неправомерное изменение схемы БД	Несанкционированное создание, изменение или удаление объектов базы данных (таблиц, представлений, процедур).	7
8	Утечка информации через побочные каналы	Несанкционированное получение информации за счет анализа побочных эффектов работы системы (время отклика, электромагнитное излучение).	5
9	Нарушение регламента резервного копирования	Сбой или намеренное нарушение процесса резервного копирования, ведущее к невозможности восстановления данных.	6
10	Несанкционированный доступ к файлам резервных копий	Хищение или копирование файлов резервных копий базы данных.	7
11	Отказ аппаратного обеспечения	Выход из строя оборудования сервера (дисковый массив, память, процессор), ведущий к недоступности БД.	5
12	Несанкционированное использование привилегий	Использование легальных высоких привилегий для совершения несанкционированных действий (например, администратором).	8
13	Перехват данных в канале связи	Несанкционированный перехват информации, передаваемой между клиентским приложением и сервером БД.	6
14	Нарушение целостности транзакций	Намеренное или случайное нарушение логики транзакций, приводящее к несогласованности данных.	6
15	Несанкционированный доступ к журналам аудита	Получение доступа к журналам регистрации событий безопасности для сокрытия других атак.	5
16	Неправомерное восстановление данных	Восстановление данных из резервной копии в обход установленных процедур, что может привести к потере актуальных данных.	5

17	Внедрение вредоносного ПО на уровне ОС	Установка на сервер БД вредоносных программ (трояны, шпионское ПО), нарушающих политику безопасности.	8
18	Несанкционированное создание учетных записей	Создание в СУБД новых учетных записей с правами доступа к данным.	6
19	Нарушение физической безопасности сервера	Прямой физический доступ к оборудованию сервера БД, позволяющий изменить его конфигурацию или похитить диски.	8
20	Неправомерное блокирование данных	Намеренная установка блокировок на данные или объекты БД, препятствующая работе легитимных пользователей.	5
21	Несанкционированное использование служебных утилит	Использование административных утилит СУБД или ОС для обхода механизмов защиты и несанкционированного доступа к данным.	7
22	Недостатки в системе управления доступом	Ошибки в настройке или проектировании системы разграничения прав доступа, позволяющие нарушителю получить несанкционированные привилегии.	6
23	Нарушение регламента обслуживания	Несоблюдение установленных процедур и регламентов по обслуживанию БД (например, установка патчей), ведущее к появлению уязвимостей.	5
24	Несанкционированное подключение к административным интерфейсам	Доступ к интерфейсам удаленного администрирования СУБД или ОС сервера БД.	7
25	Потеря или хищение носителей информации	Утрата или кража физических носителей (жестких дисков, лент), на которых хранится база данных или ее резервные копии.	6

Таблица 4 - Оценки эксперта 3, при методе непосредственной оценки

Сводная таблица							
№ УБИ	Название УБИ	Эксперт 1	Эксперт 2	Эксперт 3	Средний балл	Включено в топ-12	Ранг
5	Внедрение вредоносного кода (SQL-инъекция)	9	8	9	8,67	Да	1
2	Несанкционированная модификация данных	8	9	8	8,33	Да	2
6	Компрометация учетных данных	9	8	8	8,33	Да	3
19	Нарушение физической безопасности сервера	9	8	8	8,33	Да	4
1	Несанкционированный доступ к данным БД	9	8	7	8,00	Да	5
3	Отказ в обслуживании (DoS/DDoS)	7	9	8	8,00	Да	6
12	Несанкционированное использование привилегий	8	8	8	8,00	Да	7
17	Внедрение вредоносного ПО на уровне ОС	8	8	8	8,00	Да	8
24	Несанкционированное подключение к административным интерфейсам	8	8	7	7,67	Да	9
4	Несанкционированный доступ к конфигурации СУБД	8	7	7	7,33	Да	10
7	Неправомерное изменение схемы БД	7	8	7	7,33	Да	11
10	Несанкционированный доступ к файлам резервных копий	8	7	7	7,33	Да	12
21	Несанкционированное использование служебных утилит	7	7	7	7,00	Нет	13
18	Несанкционированное создание учетных записей	7	7	6	6,67	Нет	14
9	Нарушение регламента резервного копирования	5	8	6	6,33	Нет	15
13	Перехват данных в канале связи	7	6	6	6,33	Нет	16
14	Нарушение целостности транзакций	6	7	6	6,33	Нет	17
22	Недостатки в системе управления доступом	6	7	6	6,33	Нет	18
25	Потеря или хищение носителей информации	7	6	6	6,33	Нет	19
16	Неправомерное восстановление данных	6	6	5	5,67	Нет	20
8	Утечка информации через побочные каналы	6	5	5	5,33	Нет	21
11	Отказ аппаратного обеспечения	4	7	5	5,33	Нет	22
15	Несанкционированный доступ к журналам аудита	5	6	5	5,33	Нет	23

20	Неправомерное блокирование данных	5	6	5	5,33	Нет	24
23	Нарушение регламента обслуживания	5	6	5	5,33	Нет	25

Таблица 5 - Итоговый топ угроз по методу непосредственной оценки

Метод ранжирования

Сопроводительный текст для таблиц.

«Уважаемый эксперт, для работы Вам представлен набор угроз ИБ сервера базы данных предприятия ООО «Финмониторинг», функционирующего в сфере оказания финансовых услуг и автоматизации бухгалтерского учета. Просим Вас оценить возможность реализации каждой из обозначенных угроз ИБ на информационно-аналитическую систему предприятия и отразить свое мнение в таблице:

№ УБИ	Название УБИ	Ранг (1-25)
		1

Шкала для оценивания [1,25], где

Ранг 1 - наиболее критичная угроза

Ранг 25 - наименее критичная угроза»

Эксперт 1		
№ УБИ	Название УБИ	Ранг (1-25)
6	Компрометация учетных данных	1
5	Внедрение вредоносного кода (SQL-инъекция)	2
2	Несанкционированная модификация данных	3
19	Нарушение физической безопасности сервера	4
1	Несанкционированный доступ к данным БД	5
3	Отказ в обслуживании (DoS/DDoS)	6
17	Внедрение вредоносного ПО на уровне ОС	7
12	Несанкционированное использование привилегий	8
4	Несанкционированный доступ к конфигурации СУБД	9
24	Несанкционированное подключение к административным интерфейсам	10
10	Несанкционированный доступ к файлам резервных копий	11
7	Неправомерное изменение схемы БД	12
21	Несанкционированное использование служебных утилит	13
18	Несанкционированное создание учетных записей	14
13	Перехват данных в канале связи	15
9	Нарушение регламента резервного копирования	16
14	Нарушение целостности транзакций	17
22	Недостатки в системе управления доступом	18
25	Потеря или хищение носителей информации	19
16	Неправомерное восстановление данных	20
8	Утечка информации через побочные каналы	21
11	Отказ аппаратного обеспечения	22
15	Несанкционированный доступ к журналам аудита	23
20	Неправомерное блокирование данных	24
23	Нарушение регламента обслуживания	25

Таблица 6 - Оценка эксперта 1 при методе ранжирования

Эксперт 2		
№ УБИ	Название УБИ	Ранг (1-25)
5	Внедрение вредоносного кода (SQL-инъекция)	1
3	Отказ в обслуживании (DoS/DDoS)	2
2	Несанкционированная модификация данных	3
6	Компрометация учетных данных	4
17	Внедрение вредоносного ПО на уровне ОС	5
1	Несанкционированный доступ к данным БД	6
12	Несанкционированное использование привилегий	7
19	Нарушение физической безопасности сервера	8
7	Неправомерное изменение схемы БД	9
24	Несанкционированное подключение к административным интерфейсам	10
4	Несанкционированный доступ к конфигурации СУБД	11
9	Нарушение регламента резервного копирования	12
10	Несанкционированный доступ к файлам резервных копий	13
21	Несанкционированное использование служебных утилит	14
18	Несанкционированное создание учетных записей	15
22	Недостатки в системе управления доступом	16
11	Отказ аппаратного обеспечения	17
13	Перехват данных в канале связи	18
14	Нарушение целостности транзакций	19
25	Потеря или хищение носителей информации	20
16	Неправомерное восстановление данных	21
8	Утечка информации через побочные каналы	22
15	Несанкционированный доступ к журналам аудита	23
23	Нарушение регламента обслуживания	24
20	Неправомерное блокирование данных	25

Таблица 7 - Оценка эксперта 2 при методе ранжирования

Эксперт 3		
№ УБИ	Название УБИ	Ранг (1-25)
2	Несанкционированная модификация данных	1
5	Внедрение вредоносного кода (SQL-инъекция)	2
6	Компрометация учетных данных	3
1	Несанкционированный доступ к данным БД	4
19	Нарушение физической безопасности сервера	5
3	Отказ в обслуживании (DoS/DDoS)	6
12	Несанкционированное использование привилегий	7
17	Внедрение вредоносного ПО на уровне ОС	8
4	Несанкционированный доступ к конфигурации СУБД	9
7	Неправомерное изменение схемы БД	10
24	Несанкционированное подключение к административным интерфейсам	11
10	Несанкционированный доступ к файлам резервных копий	12
18	Несанкционированное создание учетных записей	13
21	Несанкционированное использование служебных утилит	14
13	Перехват данных в канале связи	15
14	Нарушение целостности транзакций	16
22	Недостатки в системе управления доступом	17
9	Нарушение регламента резервного копирования	18
25	Потеря или хищение носителей информации	19
16	Неправомерное восстановление данных	20
8	Утечка информации через побочные каналы	21
11	Отказ аппаратного обеспечения	22
15	Несанкционированный доступ к журналам аудита	23
20	Неправомерное блокирование данных	24
23	Нарушение регламента обслуживания	25

Таблица 8 - Оценка эксперта 3 при методе ранжирования

Итоговая таблица							
№ УБИ	Название УБИ	Ранг эксперт 1	Ранг эксперт 2	Ранг эксперт 3	Средний ранг	Включено в топ-12	Ранг
5	Внедрение вредоносного кода (SQL-инъекция)	2	1	2	1,67	Да	1
2	Несанкционированная модификация данных	3	3	1	2,33	Да	2
6	Компрометация учетных данных	1	4	3	2,67	Да	3
1	Несанкционированный доступ к данным БД	5	6	4	5,00	Да	4
3	Отказ в обслуживании (DoS/DDoS)	6	2	6	4,67	Да	5
19	Нарушение физической безопасности сервера	4	8	5	5,67	Да	6
17	Внедрение вредоносного ПО на уровне ОС	7	5	8	6,67	Да	7
12	Несанкционированное использование привилегий	8	7	7	7,33	Да	8
4	Несанкционированный доступ к конфигурации СУБД	9	11	9	9,67	Да	9
7	Неправомерное изменение схемы БД	12	9	10	10,33	Да	10
24	Несанкционированное подключение к административным интерфейсам	10	10	11	10,33	Да	11
10	Несанкционированный доступ к файлам резервных копий	11	13	12	12,00	Да	12
21	Несанкционированное использование служебных утилит	13	14	14	13,67	Нет	13
18	Несанкционированное создание учетных записей	14	15	13	14,00	Нет	14
9	Нарушение регламента резервного копирования	16	12	18	15,33	Нет	15
13	Перехват данных в канале связи	15	18	15	16,00	Нет	16
14	Нарушение целостности транзакций	17	19	16	17,33	Нет	17
22	Недостатки в системе управления доступом	18	16	17	17,00	Нет	18
25	Потеря или хищение носителей информации	19	20	19	19,33	Нет	19
16	Неправомерное восстановление данных	20	21	20	20,33	Нет	20
8	Утечка информации через побочные каналы	21	22	21	21,33	Нет	21
11	Отказ аппаратного обеспечения	22	17	22	20,33	Нет	22

15	Несанкционированный доступ к журналам аудита	23	23	23	23,00	Нет	23
20	Неправомерное блокирование данных	24	25	24	24,33	Нет	24
23	Нарушение регламента обслуживания	25	24	25	24,67	Нет	25

Таблица 9 - Итоговый список угроз по методу ранжирования

Метод парного сравнения

«Уважаемый эксперт, для работы Вам представлен набор угроз ИБ сервера базы данных предприятия ООО «Финмониторинг», функционирующего в сфере оказания финансовых услуг и автоматизации бухгалтерского учета. Просим Вас оценить возможность реализации каждой из обозначенных угроз ИБ на информационно-аналитическую систему предприятия и отразить свое мнение в таблице:

Эксперт Х	Угроза 1	Угроза 2	…	Угроза 25
Угроза 1	1			
Угроза 2	p_{ij}^{m}	1		
….				
Угроза 25				1

Шкала для оценивания

$$p_{ij}^{m} = \begin{cases} 1, \text{ если угроза } p_i \text{ равнозначна угрозе } p_j \\ 0, \text{ если угроза } p_i \text{ менее значима чем угроза } p_j \text{ »} \\ 2, \text{ если угроза } p_i \text{ более значима чем угроза } p_j \end{cases}$$

Эксперт1	Угроза1	Угроза2	Угроза3	Угроза4	Угроза5	Угроза6	Угроза7	Угроза8	Угроза9	Угроза10	Угроза11	Угроза12	Угроза13	Угроза14	Угроза15	Угроза16	Угроза17	Угроза18	Угроза19	Угроза20	Угроза21	Угроза22	Угроза23	Угроза24	Угроза25
Угроза1	1	0	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угроза2	2	1	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угроза3	0	0	1	0	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угроза4	0	0	2	1	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угроза5	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Угроза6	2	2	2	2	0	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Уг	0	0	0	0	0	0	1	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2

розa7																									
Угрозa8	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa9	0	0	0	0	0	0	0	0	1	0	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa10	0	0	0	0	0	0	0	2	2	1	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa11	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa12	2	2	2	2	0	0	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2
Угрозa13	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	0	2	0	2	2	2	2	2	2

Угроза14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	0	2	0	2	2	2	2	2	2
Угроза15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	2	2
Угроза16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	2	2	2	2	2	2
Угроза17	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	1	2	2	2	2	2	2	2	2
Угроза18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	2	2
Угроза19	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	1	2	2	2	2	2	2
Угро	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	2

за20																									
Угроза21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2
Угроза22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2
Угроза23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2
Угроза24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2
Угроза25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Таблица 10 - Оценки эксперта 1 при методе парных сравнений

Эксперт2	угроза1	угроза2	угроза3	угроза4	угроза5	угроза6	угроза7	угроза8	угроза9	угроза10	угроза11	угроза12	угроза13	угроза14	угроза15	угроза16	угроза17	угроза18	угроза19	угроза20	угроза21	угроза22	угроза23	угроза24	угроза25
угроза1	1	0	0	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза2	2	1	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза3	2	0	1	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза4	0	0	0	1	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза5	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
угроза6	2	2	2	2	0	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
уг	0	0	0	0	0	0	1	2	0	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2

розa7																									
Угрозa8	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa9	0	0	0	0	0	0	2	0	1	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa10	0	0	0	0	0	0	0	2	0	1	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa11	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa12	2	2	2	2	0	0	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2
Угрозa13	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	0	2	0	2	2	2	2	2	2

Угроза14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	0	2	0	2	2	2	2	2	2
Угроза15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	2	2
Угроза16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	2	2	2	2	2	2
Угроза17	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	1	2	2	2	2	2	2	2	2
Угроза18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	2	2
Угроза19	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	1	2	2	2	2	2	2
Угро	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	2

за20																										
Угроза21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	
Угроза22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	
Угроза23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	
Угроза24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	
Угроза25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	

Таблица 11 - Оценки эксперта 2 при методе парных сравнений

Эксперт3	угроза1	угроза2	угроза3	угроза4	угроза5	угроза6	угроза7	угроза8	угроза9	угроза10	угроза11	угроза12	угроза13	угроза14	угроза15	угроза16	угроза17	угроза18	угроза19	угроза20	угроза21	угроза22	угроза23	угроза24	угроза25
угроза1	1	0	0	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза2	2	1	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза3	2	0	1	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза4	0	0	0	1	0	0	2	2	2	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
угроза5	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
угроза6	2	2	2	2	0	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
уг	0	0	0	0	0	0	1	2	0	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2

розa7																									
Угрозa8	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa9	0	0	0	0	0	0	2	0	1	2	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa10	0	0	0	0	0	0	0	2	0	1	2	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa11	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	0	2	0	2	2	2	2	2	2
Угрозa12	2	2	2	2	0	0	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2
Угрозa13	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	0	2	0	2	2	2	2	2	2

Угроза14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	0	2	0	2	2	2	2	2	2
Угроза15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	2	2
Угроза16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	2	2	2	2	2	2
Угроза17	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	1	2	2	2	2	2	2	2	2
Угроза18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	2	2
Угроза19	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	1	2	2	2	2	2	2
Угро	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	2

за20																										
Угроза21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	
Угроза22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	
Угроза23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	
Угроза24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	
Угроза25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	

Таблица 12 - Оценки эксперта 3 при методе парных сравнений

Итоговая таблица								
№ УБИ	Название УБИ	Сумма баллов эксперт 1	Сумма баллов эксперт 2	Сумма баллов эксперт 3	Общая сумма	Средний балл	Включено в топ-12	Ранг
5	Внедрение вредоносного кода (SQL-инъекция)	48	48	48	144	48.00	Да	1
6	Компрометация учетных данных	46	46	46	138	46.00	Да	2
2	Несанкционированная модификация данных	42	42	42	126	42.00	Да	3
1	Несанкционированный доступ к данным БД	40	40	40	120	40.00	Да	4
19	Нарушение физической безопасности сервера	40	40	40	120	40.00	Да	5
12	Несанкционированное использование привилегий	40	40	40	120	40.00	Да	6
17	Внедрение вредоносного ПО на уровне ОС	40	40	40	120	40.00	Да	7
3	Отказ в обслуживании (DoS/DDoS)	38	38	38	114	38.00	Да	8
4	Несанкционированный доступ к конфигурации СУБД	38	38	38	114	38.00	Да	9
7	Неправомерное изменение схемы БД	36	36	36	108	36.00	Да	10
10	Несанкционированный доступ к файлам резервных копий	36	36	36	108	36.00	Да	11
24	Несанкционированное подключение к административным интерфейсам	34	34	34	102	34.00	Да	12
21	Несанкционированное использование служебных утилит	32	32	32	96	32.00	Нет	13
18	Несанкционированное создание учетных записей	30	30	30	90	30.00	Нет	14
9	Нарушение регламента резервного копирования	28	28	28	84	28.00	Нет	15
13	Перехват данных в канале связи	26	26	26	78	26.00	Нет	16
14	Нарушение целостности транзакций	24	24	24	72	24.00	Нет	17
22	Недостатки в системе управления доступом	22	22	22	66	22.00	Нет	18
25	Потеря или хищение носителей информации	20	20	20	60	20.00	Нет	19

16	Неправомерное восстановление данных	18	18	18	54	18.00	Нет	20
8	Утечка информации через побочные каналы	16	16	16	48	16.00	Нет	21
11	Отказ аппаратного обеспечения	14	14	14	42	14.00	Нет	22
15	Несанкционированный доступ к журналам аудита	12	12	12	36	12.00	Нет	23
20	Неправомерное блокирование данных	10	10	10	30	10.00	Нет	24
23	Нарушение регламента обслуживания	8	8	8	24	8.00	Нет	25

Таблица 13 - Итоговая оценка экспертов в методе парных сравнений

Дерево угроз

На основании рангов полученных в каждом из методов была сформирована итоговая таблица, выделяющая 6 наиболее опасных угроз.

№ УБИ	Название УБИ	Ранг метод непосредств. оценки	Ранг метод ранжирования	Ранг метод попарного сравнения	Итоговый балл	Итоговый ранг	Включено в топ-6
5	Внедрение вредоносного кода (SQL-инъекция)	1	1	1	3	1	Да
2	Несанкционированная модификация данных	2	2	3	7	2	Да
6	Компрометация учетных данных	3	3	2	8	3	Да
1	Несанкционированный доступ к данным БД	5	4	4	13	4	Да
19	Нарушение физической безопасности сервера	4	6	5	15	5	Да
3	Отказ в обслуживании (DoS/DDoS)	6	5	8	19	6	Да
12	Несанкционированное использование привилегий	7	8	6	21	7	Нет
17	Внедрение вредоносного ПО на уровне ОС	8	7	7	22	8	Нет
4	Несанкционированный доступ к конфигурации СУБД	10	9	9	28	9	Нет
7	Неправомерное изменение схемы БД	11	10	10	31	10	Нет
24	Несанкционированное подключение к административным интерфейсам	9	11	12	32	11	Нет
10	Несанкционированный доступ к файлам резервных копий	12	12	11	35	12	Нет

Таблица 14 - Итоговая таблица угроз

Модель угроз представлена на рисунке 1.

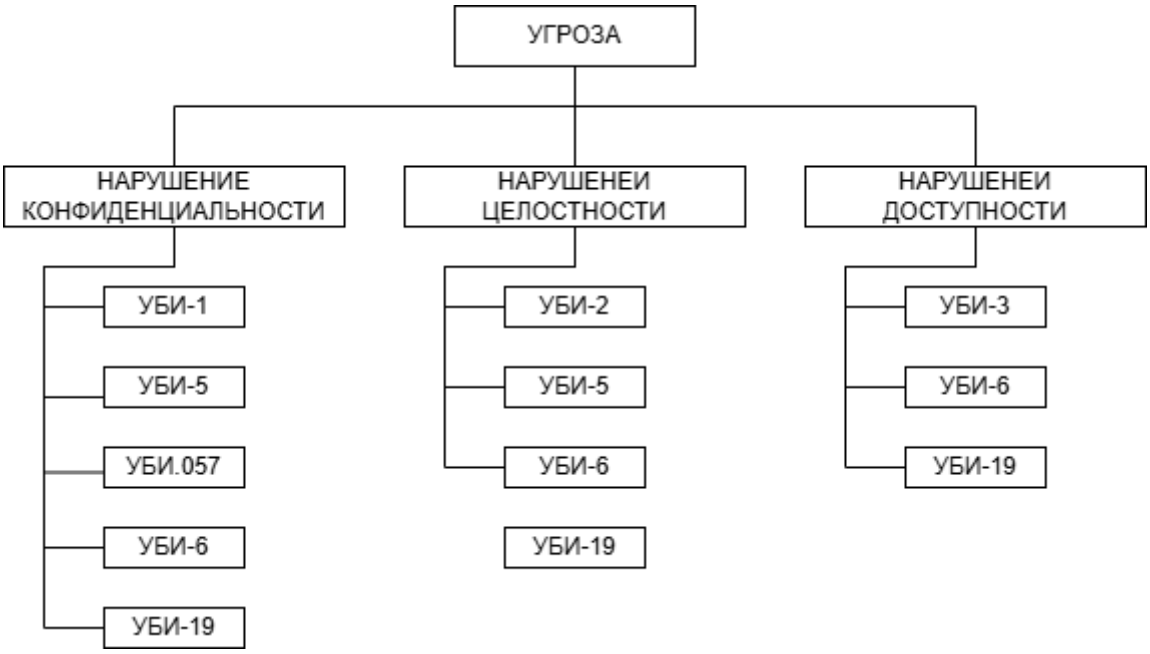

Рисунок 1 - Дерево угроз

Источники

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2018. – 8 с.
2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: Стандартинформ, 2018. – 16 с.
3. Банк данных угроз безопасности информации: ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.
4. Федеральная служба безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: www.fsb.ru.
5. Федеральная служба по техническому и экспортному контролю России [Электронный ресурс]. – Режим доступа: https://fstec.ru.