#### 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.

# Оглавление

Оглавление	2
Задание	3
Метод непосредственной оценки	7
Метод ранжирования	16
Метод парного сравнения	22
Дерево угроз	37
Источники	39

## 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.

				Наруш	Нару	Нару
			Нарушите	ение	шен	шен
№			ль и его	конфи	ие	ие
У			уровень	денци	цело	дост
Б			возможно	альнос	стно	упно
И	Название УБИ	Описание	стей	ТИ	сти	сти
	Trasbarrie v Bii		Внутренн	111	<b>V</b> 111	<b>V</b> 111
			ий/внешни			
			й			
	Несанкционир	Получение пользователем или	нарушите			
	ованный	процессом доступа к данным,	ль,			
	доступ к	не разрешенным политикой	средний			
1	данным БД	безопасности.	уровень	Да	Нет	Нет
1	данным од	ocsonachoeth.	Внутренн	да	1101	1101
			ий			
	Несанкционир	Изменение, удаление или	нарушите			
	ованная	подмена данных в базе данных	ль,			
	модификация	без соответствующих	высокий			
2	данных	полномочий.	уровень	Нет	Да	Нет
	данных	Создание условий, при	Внешний	1101	да	1101
		которых легитимные	нарушите			
	Отказ в	пользователи лишаются	ль,			
	обслуживании	доступа к серверу БД из-за	высокий			
3	(DoS/DDoS)	исчерпания ресурсов.	уровень	Нет	Нет	Да
	(DOS/DDOS)	пе терпатия ресурсов.	Внутренн	1101	1101	Ди
	Несанкционир		ий			
	ованный	Изменение параметров	нарушите			
	доступ к	конфигурации сервера БД,	ль,			
	конфигурации	ведущее к снижению уровня	высокий			
4	СУБД	безопасности.	уровень	Да	Да	Да
	~ · · · · · · · · · · · · · · · · · · ·	occontaction.	Внешний	Д"	Ди	ди
	Внедрение	Внедрение и выполнение	нарушите			
	вредоносного	произвольного SQL-кода через	ль,			
	кода (SQL-	уязвимости в клиентских	средний			
5	инъекция)	приложениях.	уровень	Да	Да	Нет
	ппьскции)	приложениях.	Внутренн	Ди	Ди	1101
		Хищение или подбор учетных	ий/внешни			
	Компрометаци	данных (логинов/паролей)	й			
	я учетных	легитимных пользователей или	нарушите			
6	данных	администраторов БД.	ль,	Да	Да	Да
	данных	администраторов од.	ль,	Да	Да	да

			opo HIIII			
			средний			
-			уровень			
		11	Внутренн			
		Несанкционированное	ий			
	TT	создание, изменение или	нарушите			
	Неправомерно	удаление объектов базы	ль,			
7	е изменение	данных (таблиц,	высокий	11	п	11
7	схемы БД	представлений, процедур).	уровень	Нет	Да	Нет
	<b>V</b>	Несанкционированное	D			
	Утечка	получение информации за счет	Внешний			
	информации	анализа побочных эффектов	нарушите			
	через	работы системы (время	ль,			
0	побочные	отклика, электромагнитное	высокий	п	TT	11
8	каналы	излучение).	уровень	Да	Нет	Нет
	**	Сбой или намеренное	Внутренн			
	Нарушение	нарушение процесса	ий			
	регламента	резервного копирования,	нарушите			
	резервного	ведущее к невозможности	ль, низкий			_
9	копирования	восстановления данных.	уровень	Нет	Нет	Да
	Несанкционир		Внутренн			
	ованный		ий			
	доступ к		нарушите			
	файлам	Хищение или копирование	ль,			
1	резервных	файлов резервных копий базы	средний			
0	копий	данных.	уровень	Да	Нет	Нет
			Техногенн			
		Выход из строя оборудования	ый фактор			
	Отказ	сервера (дисковый массив,	(не			
1	аппаратного	память, процессор), ведущий к	нарушите			
1	обеспечения	недоступности БД.	ль)	Нет	Нет	Да
		Использование легальных	Внутренн			
		высоких привилегий для	ий			
	Несанкционир	совершения	нарушите			
	ованное	несанкционированных	ль,			
1	использование	действий (например,	высокий			
2	привилегий	администратором).	уровень	Да	Да	Нет
		Несанкционированный	Внешний			
		перехват информации,	нарушите			
	Перехват	передаваемой между	ль,			
1	данных в	клиентским приложением и	средний			
3	канале связи	сервером БД.	уровень	Да	Нет	Нет
			Внутренн			
			ий			
		Намеренное или случайное	нарушите			
	Нарушение	нарушение логики транзакций,	ль,			
1	целостности	приводящее к	средний			
4	транзакций	несогласованности данных.	уровень	Нет	Да	Нет
	Несанкционир	77				
	ованный	Получение доступа к журналам	Внутренн			
	доступ к	регистрации событий	ий			
1	журналам	безопасности для сокрытия	нарушите			
5	аудита	других атак.	ль,	Да	Нет	Нет
	мудина	других шик.	,1D,	<sub>  Д</sub> и	1101	1101

					T	
			средний			
			уровень			
		D	Внутренн			
	TT	Восстановление данных из	ий			
	Неправомерно	резервной копии в обход	нарушите			
	e	установленных процедур, что	ль,			
1	восстановлени	может привести к потере	средний		<b> </b>	
6	е данных	актуальных данных.	уровень	Нет	Да	Нет
		Установка на сервер БД	Внешний			
	Внедрение	вредоносных программ	нарушите			
	вредоносного	(трояны, шпионское ПО),	ль,			
1	ПО на уровне	нарушающих политику	высокий			
7	OC	безопасности.	уровень	Да	Да	Да
			Внутренн			
	Несанкционир		ий			
	ованное		нарушите			
	создание	Создание в СУБД новых	ль,			
1	учетных	учетных записей с правами	высокий			
8	записей	доступа к данным.	уровень	Да	Да	Нет
		Прямой физический доступ к	Внутренн		C	1
	Нарушение	оборудованию сервера БД,	ий			
	физической	позволяющий изменить его	нарушите			
1	безопасности	конфигурацию или похитить	ль, низкий			
9	сервера	диски.	уровень	Да	Да	Да
	сервера	диски.	• •	да	да	Да
		<b>Поморомной можеморие</b>	Внутренн ий			
	Harmanaya	Намеренная установка				
	Неправомерно	блокировок на данные или	нарушите			
	e	объекты БД, препятствующая	ль,			
2	блокирование	работе легитимных	средний	**		П П
0	данных	пользователей.	уровень	Нет	Нет	Да
	**	Использование	Внутренн			
	Несанкционир	административных утилит	ий			
	ованное	СУБД или ОС для обхода	нарушите			
	использование	механизмов защиты и	ль,			
2	служебных	несанкционированного доступа	высокий			
1	утилит	к данным.	уровень	Да	Да	Нет
		Ошибки в настройке или				
		проектировании системы	Внутренн			
		разграничения прав доступа,	ий			
	Недостатки в	позволяющие нарушителю	нарушите			
	системе	получить	ль,			
2	управления	несанкционированные	средний			
2	доступом	привилегии.	уровень	Да	Да	Нет
	-	Несоблюдение установленных	Внутренн			
		процедур и регламентов по	ий			
	Нарушение	обслуживанию БД (например,	нарушите			
2	регламента	установка патчей), ведущее к	ль, низкий			
3	обслуживания	появлению уязвимостей.	уровень	Нет	Да	Да
	Несанкционир	Доступ к интерфейсам	71			F 1
	ованное	удаленного	Внешний			
2	подключение	администрирования СУБД или	нарушите			
4	К	ОС сервера БД.	ль,	Да	Да	Да
	IV.	ос сервера вд.	ль,	Да	Да	да

	администрати		высокий			
	вным		уровень			
	интерфейсам					
			Внутренн			
		Утрата или кража физических	ий/внешни			
	Потеря или	носителей (жестких дисков,	й			
	хищение	лент), на которых хранится	нарушите			
2	носителей	база данных или ее резервные	ль, низкий			
5	информации	копии.	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:

№ УБІ	1   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.

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

	Внедрение	Установка на сервер БД вредоносных программ	
	вредоносного ПО на	(трояны, шпионское ПО), нарушающих политику	ı
17	уровне ОС	безопасности.	8
	Несанкционированное		
	создание учетных	Создание в СУБД новых учетных записей с	
18	записей	правами доступа к данным.	7
		Прямой физический доступ к оборудованию	
	Нарушение физической	сервера БД, позволяющий изменить его	
19	безопасности сервера	конфигурацию или похитить диски.	9
		Намеренная установка блокировок на данные или	
	Неправомерное	объекты БД, препятствующая работе легитимных	
20	блокирование данных	пользователей.	5
	Несанкционированное	Использование административных утилит СУБД	
	использование	или ОС для обхода механизмов защиты и	
21	служебных утилит	несанкционированного доступа к данным.	7
		Ошибки в настройке или проектировании системы	
		разграничения прав доступа, позволяющие	
	Недостатки в системе	нарушителю получить несанкционированные	
22	управления доступом	привилегии.	6
		Несоблюдение установленных процедур и	
		регламентов по обслуживанию БД (например,	
	Нарушение регламента	установка патчей), ведущее к появлению	
23	обслуживания	уязвимостей.	5
	Несанкционированное		1
	подключение к		
	административным	Доступ к интерфейсам удаленного	.
24	интерфейсам	администрирования СУБД или ОС сервера БД.	8
		Утрата или кража физических носителей (жестких	
	Потеря или хищение	дисков, лент), на которых хранится база данных	.
25	носителей информации	или ее резервные копии.	7

Таблица 2 - Оценки эксперта 1, при методе непосредственной оценки

No			Оце
У			нка
Б			(1-
И	Название УБИ	Описание	10)
		Получение пользователем или процессом доступа	- /
	Несанкционированный	к данным, не разрешенным политикой	
1	доступ к данным БД	безопасности.	8
	Несанкционированная	Изменение, удаление или подмена данных в базе	
2	модификация данных	данных без соответствующих полномочий.	9
		Создание условий, при которых легитимные	
	Отказ в обслуживании	пользователи лишаются доступа к серверу БД из-	
3	(DoS/DDoS)	за исчерпания ресурсов.	9
	Несанкционированный	1 71	
	доступ к конфигурации	Изменение параметров конфигурации сервера БД,	
4	СУБД	ведущее к снижению уровня безопасности.	7
	Внедрение		
	вредоносного кода	Внедрение и выполнение произвольного SQL-кода	
5	(SQL-инъекция)	через уязвимости в клиентских приложениях.	8
		Хищение или подбор учетных данных	
	Компрометация	(логинов/паролей) легитимных пользователей или	
6	учетных данных	администраторов БД.	8
		Несанкционированное создание, изменение или	
	Неправомерное	удаление объектов базы данных (таблиц,	
7	изменение схемы БД	представлений, процедур).	8
	, ,	Несанкционированное получение информации за	
	Утечка информации	счет анализа побочных эффектов работы системы	
8	через побочные каналы	(время отклика, электромагнитное излучение).	5
	Нарушение регламента	Сбой или намеренное нарушение процесса	
	резервного	резервного копирования, ведущее к	
9	копирования	невозможности восстановления данных.	8
	Несанкционированный		
	доступ к файлам	Хищение или копирование файлов резервных	
10	резервных копий	копий базы данных.	7
		Выход из строя оборудования сервера (дисковый	
	Отказ аппаратного	массив, память, процессор), ведущий к	
11	обеспечения	недоступности БД.	7
	Несанкционированное	Использование легальных высоких привилегий	
	использование	для совершения несанкционированных действий	
12	привилегий	(например, администратором).	8
		Несанкционированный перехват информации,	
	Перехват данных в	передаваемой между клиентским приложением и	
13	канале связи	сервером БД.	6
	Нарушение	Намеренное или случайное нарушение логики	
	целостности	транзакций, приводящее к несогласованности	
14	транзакций	данных.	7
	Несанкционированный		
	доступ к журналам	Получение доступа к журналам регистрации	
15	аудита	событий безопасности для сокрытия других атак.	6
	**	Восстановление данных из резервной копии в	
	Неправомерное	обход установленных процедур, что может	
16	восстановление данных	привести к потере актуальных данных.	6

	Внедрение	Установка на сервер БД вредоносных программ	1
	вредоносного ПО на	(трояны, шпионское ПО), нарушающих политику	i
17	уровне ОС	безопасности.	8
	Несанкционированное		
	создание учетных	Создание в СУБД новых учетных записей с	1
18	записей	правами доступа к данным.	7
		Прямой физический доступ к оборудованию	1
	Нарушение физической	сервера БД, позволяющий изменить его	1
19	безопасности сервера	конфигурацию или похитить диски.	8
		Намеренная установка блокировок на данные или	
	Неправомерное	объекты БД, препятствующая работе легитимных	
20	блокирование данных	пользователей.	6
	Несанкционированное	Использование административных утилит СУБД	
	использование	или ОС для обхода механизмов защиты и	1
21	служебных утилит	несанкционированного доступа к данным.	7
		Ошибки в настройке или проектировании системы	
		разграничения прав доступа, позволяющие	
	Недостатки в системе	нарушителю получить несанкционированные	1
22	управления доступом	привилегии.	7
		Несоблюдение установленных процедур и	
		регламентов по обслуживанию БД (например,	
	Нарушение регламента	установка патчей), ведущее к появлению	
23	обслуживания	уязвимостей.	6
	Несанкционированное		
	подключение к		
	административным	Доступ к интерфейсам удаленного	
24	интерфейсам	администрирования СУБД или ОС сервера БД.	8
		Утрата или кража физических носителей (жестких	
	Потеря или хищение	дисков, лент), на которых хранится база данных	
25	носителей информации	или ее резервные копии.	6

Таблица 3 - Оценки эксперта 2, при методе непосредственной оценки

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

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

Таблица 4 - Оценки эксперта 3, при методе непосредственной оценки

	Сводна	я табли	ща				
No					Средн	Включен	P
УБ		Эксп	Эксп	Эксп	ий	о в топ-	ан
И	Название УБИ	ерт 1	ерт 2	ерт 3	балл	12	Γ
	Внедрение вредоносного кода						
5	(SQL-инъекция)	9	8	9	8,67	Да	1
	Несанкционированная						
2	модификация данных	8	9	8	8,33	Да	2
6	Компрометация учетных данных	9	8	8	8,33	Да	3
	Нарушение физической						
19	безопасности сервера	9	8	8	8,33	Да	4
	Несанкционированный доступ к						
1	данным БД	9	8	7	8,00	Да	5
3	Отказ в обслуживании (DoS/DDoS)	7	9	8	8,00	Да	6
	Несанкционированное						
12	использование привилегий	8	8	8	8,00	Да	7
	Внедрение вредоносного ПО на						
17	уровне ОС	8	8	8	8,00	Да	8
	Несанкционированное						
	подключение к административным						
24	интерфейсам	8	8	7	7,67	Да	9
	Несанкционированный доступ к						1
4	конфигурации СУБД	8	7	7	7,33	Да	0
	Неправомерное изменение схемы	_		_		_	1
7	БД	7	8	7	7,33	Да	1
1.0	Несанкционированный доступ к		_	_			1
10	файлам резервных копий	8	7	7	7,33	Да	2
21	Несанкционированное		_	_	7.00	**	1
21	использование служебных утилит	7	7	7	7,00	Нет	3
10	Несанкционированное создание	7	7		6.67	II.	1
18	учетных записей	7	7	6	6,67	нет	4
9	Нарушение регламента резервного	5	8	6	6,33	Нет	1 5
9	копирования	3	0	0	0,33	1161	1
13	Перехват данных в канале связи	7	6	6	6,33	Нет	6
13	Нарушение целостности	,	0	0	0,33	1101	1
14	транзакций	6	7	6	6,33	Нет	7
1.	Недостатки в системе управления	0	,	Ü	0,00	1101	1
22	доступом	6	7	6	6,33	Нет	8
	Потеря или хищение носителей				,		1
25	информации	7	6	6	6,33	Нет	9
	Неправомерное восстановление						2
16	данных	6	6	5	5,67	Нет	0
	Утечка информации через						2
8	побочные каналы	6	5	5	5,33	Нет	1
							2
11	Отказ аппаратного обеспечения	4	7	5	5,33	Нет	2
	Несанкционированный доступ к						2
15	журналам аудита	5	6	5	5,33	Нет	3

	Неправомерное блокирование						2
20	данных	5	6	5	5,33	Нет	4
	Нарушение регламента						2
23	обслуживания	5	6	5	5,33	Нет	5

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	10
10	административным интерфейсам  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	
$N_{\underline{0}}$		Ранг (1-
УБИ	Название УБИ	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
	Несанкционированное подключение к	
24	административным интерфейсам	10
4	Несанкционированный доступ к конфигурации СУБД	11
9	Нарушение регламента резервного копирования	12
	Несанкционированный доступ к файлам резервных	
10	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	
No		Ранг (1-
УБИ	Название УБИ	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
	Несанкционированное подключение к	
24	административным интерфейсам	11
	Несанкционированный доступ к файлам резервных	
10	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

	Ито	говая таб	лица				
№ УБ И	Название УБИ	Ранг экспер т 1	Ранг экспер т 2	Ранг экспер т 3	Средн ий ранг	Включе но в топ-12	Р а н г
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	1 0
24	Несанкционированное подключение к административным интерфейсам	10	10	11	10,33	Да	1 1
10	Несанкционированный доступ к файлам резервных копий	11	13	12	12,00	Да	1 2
21	Несанкционированное использование служебных утилит	13	14	14	13,67	Нет	1 3
18	Несанкционированное создание учетных записей	14	15	13	14,00	Нет	1 4
9	Нарушение регламента резервного копирования	16	12	18	15,33	Нет	1 5
13	Перехват данных в канале связи	15	18	15	16,00	Нет	1 6
14	Нарушение целостности транзакций	17	19	16	17,33	Нет	1 7
22	Недостатки в системе управления доступом	18	16	17	17,00	Нет	1 8
25	Потеря или хищение носителей информации	19	20	19	19,33	Нет	1 9
16	Неправомерное восстановление данных	20	21	20	20,33	Нет	2 0
8	Утечка информации через побочные каналы	21	22	21	21,33	Нет	2
11	Отказ аппаратного обеспечения	22	17	22	20,33	Нет	2 2

	Несанкционированный доступ к						2
15	журналам аудита	23	23	23	23,00	Нет	3
	Неправомерное блокирование						2
20	данных	24	25	24	24,33	Нет	4
	Нарушение регламента						2
23	обслуживания	25	24	25	24,67	Нет	5

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:

	Угроза 1	Угроза 2	•••	Угроза 25
Эксперт Х				
Угроза 1	1			
Угроза 2	$p_{ij}^m$	1		
••••				
Угроза 25				1

#### Шкала для оценивания

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

Y	6	У г р о з а	У г р о з а 5	У г р о з а 4	у г р о з а з	У г р о з а 2	у г р о з а 1	Э к с п е р т
Y	2		2	0	0		1	г р о з а
Y	2		2	0	0		0	Г р о з а
Y	2		2	2	1		2	г р о з а
Y	2		2	1	0		2	г р о з
Y         Y         Y         Y         T	0		1	0	0		0	г р о з а
Y	1		2	0	0		0	г р о з а
Y	2		2	2	2		2	Г р о з а
Y         r	2		2	2	2		2	г р о з а
T         T	2		2	2	2		2	г р о з а
T         T	2		2	2	2		2	Γ p o 3 a 1
T         T	2		2	2	2		2	Γ p o 3 a 1
T         T	2		2	0	0		0	г р о з а 1
T         T	2		2	2	2		2	Γ p o 3 a 1
T         T	2		2	2	2		2	Γ p o 3 a 1
T         T	2		2	2	2		2	г р о з а 1
T         T         T         T         T         T         T         T         P	2		2	2	2		2	г р о з а 1
T         T         T         T         T         T         T         P	2		2	0	0		0	г р о з а 1
r        r       r       r       r       r       r       r       r       r       r       r       r       r       r       r        r       r       r       r       r       r       r       r       r       r       r       r       r       r       r        r	2		2	2	2		2	Γ p o 3 a 1
r       r       r       r       r       r       r       p        p       p       p       p       p       p       p       p       p       p       p       p       p       p       p        p       p       p       p       p       p       p       p       p       p       p       p       p       p       p        p       p       p       p       p       p       p       p       p       p       p       p       p       p       p        p <td>2</td> <td></td> <td>2</td> <td>0</td> <td>0</td> <td></td> <td>0</td> <td>г р о з а 1</td>	2		2	0	0		0	г р о з а 1
Г       Г       Г       Г       Р        Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р        Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р       Р        Р <td>2</td> <td></td> <td>2</td> <td>2</td> <td>2</td> <td></td> <td>2</td> <td>Γ p o 3 a 2</td>	2		2	2	2		2	Γ p o 3 a 2
Г       Г       Г       Г       Р       р       р       р       о        о       о       о       о       о       о       о       о       о       о       о       о       о       о       о        о       о       о       о       о       о       о       о       о       о       о       о       о       о       о        о <td>2</td> <td></td> <td>2</td> <td>2</td> <td>2</td> <td></td> <td>2</td> <td>Γ p o 3 a 2</td>	2		2	2	2		2	Γ p o 3 a 2
r       r       r         p       p       p         o       o       o         3       3       3         a       a       a         2       2       2         2       2       2         2       2       2         2       2       2         2       2       2         2       2       2         2       2       2         2       2       2         2       2       2         4       1       1         4       1       1         5       1       1         6       1       1         7       2       2         2       2       2         2       2       2         2       2       2         2       2       2         3       3       3         4       5         5       2       2         6       1       1         7       2       2         8       2       2         9<	2		2	2	2		2	Γ p o 3 a 2
r r p p o o o o o o o o o o o o o o o o	2		2	2	2		2	г р о з а 2
гроза 2 2 2 2	2		2	2	2		2	Γ p o 3 a 2
	2		2		2		2	Γ p o 3 a 2

У г р о з а 1 3	У г р о з а 1 2	У г р о з а 1	У г р о з а 1	У г р о з а 9	7 У г р о з а 8	р о з а
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	0	0	0	0	0	
0	0	0	0	0	0	
0	2	0	0	0	0	
0	2	0	2	0	1	
0	2	0	2	1	2	
0	2	0	1	0	0	
0	2	1	2	2	2	
0	1	0	0	0	0	
1	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	

У г р о	У г р о з а 1 9	У г р о з а 1 8	У г р о з а 1	5 У г р о з а 1 6	г р о з а 1	У г р о з а 1 4
0	2	0	2	0	0	0
0	2	0	2	0	0	0
0	2	0	2	0	0	0
0	2	0	2	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	2	0	2	0	0	0
0	2	0		0	0	0
0	2	0		0	0	0
0	2	0	2	0	0	0
0	2	0	2	0	0	0
0	0	0	0	0	0	0
0	2	0		0	0	0
0	2	0	2	0	0	1
0	2	0		0	1	2
0	2	0	2	1	2	2
0	0	0	1	0	0	0
0	2	1		2	2	2
0	1	0	2	0	0	0
1	2	2	2	2	2	2
2	2	2	2	2	2	2
2	2	2	2	2	2	2
2	2	2	2	2	2	2
2	2	2	2	2	2	2
2	2	2	2	2	2	2

3																									
a																									
0																									
У																									
Γ																									
p																									
O																									
3																									
a 2																									
1	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
У																									
Γ																									
p o																									
3																									
a																									
2 2	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
У	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	1			
Γ																									
p																									
0																									
з а																									
2 3	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
У																									
г р																									
0																									
3																									
a																									
2 4	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
У	U	U	U	J	U	U	U	J	U	0	0	U	U	U	J	0		0	0	0	0	0	0	1	
Γ																									
p																									
0																									
3 a																									
2 5																									
5	0	0	0	0	10	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

a 6	У г р о з	У г р о з а 5	У г р о з а 4	У г р о з а 3	У г р о з а 2	У г р о з а 1	Э к с п е р т
2		2	0	2	2	1	У г р о з а 1
2		2	0	0	1	0	У г р о з а 2
2		2	0	1	2	0	У г р о з а
2		2	1	2	2	2	У г р о з а 4
0		1	0	0	0	0	У г р о з а 5
1		2	0	0	0	0	У г р о з а 6
2		2	2	2	2	2	У г р о з а 7
2		2	2	2	2	2	У г р о з а 8
2		2	2	2	2	2	У г р о з а 9
2		2	2	2	2	2	У гр о з а 1
2		2	2	2	2	2	У гр о з а 1
2		2	0	0	0	0	У г р о з а 1 2
2		2	2	2	2	2	У г р о з а 1 3
2		2	2	2	2	2	У гр о з а 1
2		2	2	2	2	2	У гр о з а 1 5
2		2	2	2	2	2	У г р о з а 1 6
2		2	0	0	0	0	У г р о з а 1
2		2	2	2	2	2	У г р о з а 1 8
2		2	0	0	0	0	У г р о з а 1
2		2	2	2	2	2	У г р о з а 2
2		2	2	2	2	2	У гр о з а 2
2		2	2	2	2	2	У г р о з а 2
2		2	2	2	2	2	У гр о з а 2 3
2		2	2	2	2	2	У гр о з а 2 4
2		2	2	2	2	2	У г р о з а 2 5
			-				

У г р о з а 1 3	У г р о з а 1 2	У г р о з а 1	y Γ p o 3 a 1 0	У г р о з а 9	7 У г р о з а 8	р о з а
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	0	0	0	0	0	
0	0	0	0	0	0	
0	2	0	0	2	0	
0	2	0	2	0	1	
0	2	0	0	1	2	
0	2	0	1	2	0	
0	2	1	2	2	2	
0	1	0	0	0	0	
1	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	

3 a																									
2																									
У Г																									
p																									
0 3																									
a																									
2	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
У г																									
p																									
O 3																									
a 2																									
2 2 У	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
у Г																									
p																									
0 3																									
a 2																									
2 3 y	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
у Г																									
p o																									
3																									
a 2																									
2 4 У	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
Г																									
p o																									
3																									
a 2 5																									
5	0	0 T. (	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

г р о	<u>5</u> У	У г р о з а	У г р о з а 4	У г р о з а 3	У г р о з а 2	У г р о з а 1	Э к с п е р т
	2		0	2	2	1	У г р о з а 1
	2		0	0	1	0	У г р о з а 2
	2		0	1	2	0	У г р о з а 3
	2		1	2	2	2	У г р о з а 4
	1		0	0	0	0	У г р о з а 5
	2		0	0	0	0	У г р о з а 6
	2		2	2	2	2	У г р о з а 7
	2		2	2	2	2	У г р о з а 8
	2		2	2	2	2	У г р о з а 9
	2		2	2	2	2	У гр о з а 1
	2		2	2	2	2	У гр о з а 1
	2		0	0	0	0	У гр о з а 1 2
	2		2	2	2	2	У гр о з а 1 3
	2		2	2	2	2	У гр о з а 1 4
	2		2	2	2	2	У гр о з а 1 5
	2		2	2	2	2	У гр о з а 1
	2		0	0	0	0	У гр о з а 1
	2		2	2	2	2	У гр о з а 1 8
	2		0	0	0	0	У гр о з а 1
	2		2	2	2	2	У гр о з а 2
	2		2	2	2	2	У гр о з а 2
	2		2	2	2	2	У гр о з а 2
	2		2	2	2	2	У гр о з а 2 3
	2		2	2	2	2	У гр о з а 2 4
	2		2	2	2	2	У г р о з а 2 5

У г р о з а 1 3	У г р о з а 1 2	У г р о з а 1	y Γ p o 3 a 1 0	У г р о з а 9	7 У г р о з а 8	р о з а
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	2	0	0	0	0	
0	0	0	0	0	0	
0	0	0	0	0	0	
0	2	0	0	2	0	
0	2	0	2	0	1	
0	2	0	0	1	2	
0	2	0	1	2	0	
0	2	1	2	2	2	
0	1	0	0	0	0	
1	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
0	2	0	0	0	0	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	
2	2	2	2	2	2	

У г р о з а 1 4 У г	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	0	2	0	2	2	2	2	
о 3 а 1 5 У г р	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	0	2	2	2	2	
3 а 1 6 У г р о з а	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	2	2	2	2	
1 7 У г р о з а 1 8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	2	2	2	
У г р о з а 1 9	2	2	2	2	0	0	2	2	2	2	2	0	2	2	2	2	0	2	1	2	2	2	2	
г р о	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2

3 a 2 0																									
у г р о з а																									
2	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
У г р о з а		,			,	,						,	,	,											
2 2 У г р о з а 2 3	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
У г р о з а 2	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
У г р о з а 2 5	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

		Итого	вая таблиц	a				
№		Сумма	Сумма	Сумма	Общ	Сре		P
У		баллов	баллов	баллов	ая	дни	Вклю	a
Б		эксперт	эксперт	эксперт	сум	й	чено в	Н
И	Название УБИ	1	2	3	ма	балл	топ-12	Γ
	Внедрение вредоносного					48.0		
5	кода (SQL-инъекция)	48	48	48	144	0	Да	1
	Компрометация учетных					46.0		
6	данных	46	46	46	138	0	Да	2
	Несанкционированная					42.0		
2	модификация данных	42	42	42	126	0	Да	3
	Несанкционированный					40.0		
1	доступ к данным БД	40	40	40	120	0	Да	4
	Нарушение физической					40.0		
19	безопасности сервера	40	40	40	120	0	Да	5
	Несанкционированное						, ,	
	использование					40.0		
12	привилегий	40	40	40	120	0	Да	6
	Внедрение вредоносного					40.0		
17	ПО на уровне ОС	40	40	40	120	0	Да	7
	Отказ в обслуживании					38.0	, ,	
3	(DoS/DDoS)	38	38	38	114	0	Да	8
	Несанкционированный							
	доступ к конфигурации					38.0		
4	СУБД	38	38	38	114	0	Да	9
	Неправомерное					36.0		1
7	изменение схемы БД	36	36	36	108	0	Да	0
	Несанкционированный							
	доступ к файлам					36.0		1
10	резервных копий	36	36	36	108	0	Да	1
	Несанкционированное							
	подключение к							
	административным					34.0		1
24	интерфейсам	34	34	34	102	0	Да	2
	Несанкционированное							
	использование					32.0		1
21	служебных утилит	32	32	32	96	0	Нет	3
	Несанкционированное							
	создание учетных					30.0		1
18	записей	30	30	30	90	0	Нет	4
	Нарушение регламента					28.0		1
9	резервного копирования	28	28	28	84	0	Нет	5
	Перехват данных в					26.0		1
13	канале связи	26	26	26	78	0	Нет	6
	Нарушение целостности					24.0		1
14	транзакций	24	24	24	72	0	Нет	7
	Недостатки в системе					22.0		1
22	управления доступом	22	22	22	66	0	Нет	8
	Потеря или хищение					20.0		1
25	носителей информации	20	20	20	60	0	Нет	9

	Неправомерное					18.0		2
16	восстановление данных	18	18	18	54	0	Нет	0
	Утечка информации					16.0		2
8	через побочные каналы	16	16	16	48	0	Нет	1
	Отказ аппаратного					14.0		2
11	обеспечения	14	14	14	42	0	Нет	2
	Несанкционированный							
	доступ к журналам					12.0		2
15	аудита	12	12	12	36	0	Нет	3
	Неправомерное					10.0		2
20	блокирование данных	10	10	10	30	0	Нет	4
	Нарушение регламента							2
23	обслуживания	8	8	8	24	8.00	Нет	5

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.

No		Ранг	Ранг			Итог	Вклю
У		метод	метод	Ранг метод	Итог	овы	чено
Б		непосредс	ранжиро	попарного	овый	й	в топ-
И	Название УБИ	тв. оценки	вания	сравнения	балл	ранг	6
	Внедрение	·		•		1	
	вредоносного кода						
5	(SQL-инъекция)	1	1	1	3	1	Да
	Несанкционированная						
2	модификация данных	2	2	3	7	2	Да
	Компрометация						
6	учетных данных	3	3	2	8	3	Да
	Несанкционированный						
1	доступ к данным БД	5	4	4	13	4	Да
	Нарушение физической						
19	безопасности сервера	4	6	5	15	5	Да
	Отказ в обслуживании						
3	(DoS/DDoS)	6	5	8	19	6	Да
	Несанкционированное						
	использование						
12	привилегий	7	8	6	21	7	Нет
	Внедрение						
	вредоносного ПО на						
17	уровне ОС	8	7	7	22	8	Нет
	Несанкционированный						
	доступ к конфигурации					_	
4	СУБД	10	9	9	28	9	Нет
_	Неправомерное					1.0	
7	изменение схемы БД	11	10	10	31	10	Нет
	Несанкционированное						
	подключение к						
24	административным		1.1	12	22	1.1	
24	интерфейсам	9	11	12	32	11	Нет
	Несанкционированный						
10	доступ к файлам	10	10	1.1	25	10	11
10	резервных копий	12	12	11	35	12	Нет

Таблица 14 - Итоговая таблица угроз

## Модель угроз представлена на рисунке 1.

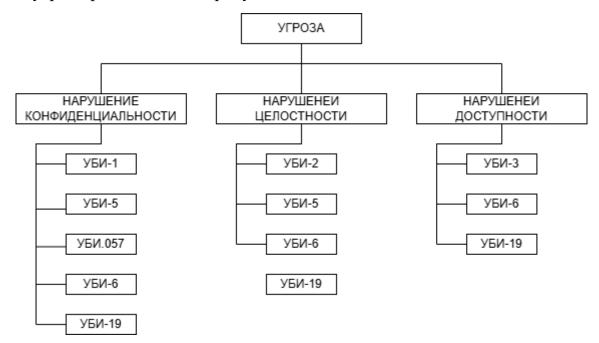


Рисунок 1 - Дерево угроз

#### 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.