

**МИНОБРНАУКИ 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 №3**

**В РАМКАХ ДИСЦИПЛИНЫ «МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ»**

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

# Оглавление

[Оглавление 2](#_Toc210998594)

[Задание 3](#_Toc210998595)

# 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.

2. Список УБИ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № УБИ | Название УБИ | Описание | Нарушитель и его уровень возможностей | Нарушение конфиденциальности | Нарушение целостности | Нарушение доступности |
| УБИ.004 | Угроза аппаратного сброса пароля BIOS | Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). | Внутренний нарушитель с низким потенциалом | НЕТ | ДА | НЕТ |
| УБИ.022 | Угроза избыточного выделения оперативной памяти | Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | ДА | НЕТ | НЕТ |
| УБИ.037 | Угроза исследования приложения через отчёты об ошибках | Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | ДА | НЕТ | НЕТ |
| УБИ.047 | Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке | Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). | Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом | НЕТ | НЕТ | ДА |
| УБИ.050 | Угроза неверного определения формата входных данных, поступающих в хранилище больших | гроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. | Внутренний нарушитель с низким потенциалом | НЕТ | ДА | НЕТ |
| УБИ.057 | Угроза неконтролируемого копирования данных внутри хранилища больших данных | Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. | Внутренний нарушитель с низким потенциалом | ДА | НЕТ | НЕТ |
| УБИ.061 | Угроза некорректного задания структуры данных транзакции | гроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. | Внутренний нарушитель со средним потенциалом | НЕТ | ДА | ДА |
| УБИ.071 | Угроза несанкционированного восстановления удалённой защищаемой информации | гроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | ДА | НЕТ | НЕТ |
| УБИ.084 | Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети | Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | ДА | ДА | ДА |
| УБИ.091 | Угроза несанкционированного удаления защищаемой информации | Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | НЕТ | НЕТ | ДА |
| УБИ.100 | Угроза обхода некорректно настроенных механизмов аутентификации | Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). | Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом | ДА | ДА | ДА |

Таблица 1 - Модель угроз

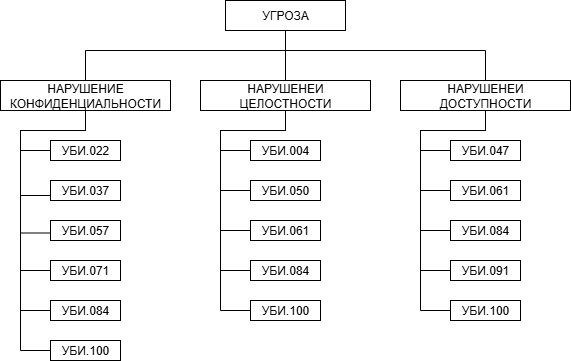


Рисунок 2 - Дерево угроз

Источники

**1.** Источник информации ФСТЭК России <http://data-sec.ru/personal-data/threats-data-bank/>  Дата обращения: 26.09.2025