**МЕТОДЫ ЗАЩИТЫ БАЗ ДАННЫХ НА ПРЕДПРИЯТИЯХ МАЛОГО БИЗНЕСА**

**Кутьин Захар Сергеевич**

**Крутов Алексей Михайлович**

**студенты 3 курса кафедры защиты информации РТУ МИРЭА, специальность информационная безопасность**

**Научный руководитель: преподаватель Шутов Василий Александрович**

***РТУ МИРЭА, Институт кибербезопасности и цифровых технологий***

***Аннотация:*** *Каждый год количество кибератак на организации разного размера увеличивается в 1,5-2 раза. Кроме того, инциденты информационной безопасности, такие как утечки информации о кредитных картах, кража личных данных, программы-вымогатели, кража интеллектуальной собственности, отказ в обслуживании, публикации в общий доступ баз данных, уже давно стали обычной новостью. Малый бизнес не готов выделять многомиллионный бюджет на свою безопасность, поскольку располагает довольно ограниченными финансовыми и людскими ресурсами. Поэтому многим предпринимателям необходимо знать несколько способов обеспечения информационной безопасности баз данных, которые можно использовать даже при ограниченных ресурсах. Некоторые из них будут рассмотрены в этой статье.*

***Ключевые слова:*** *информационная безопасность баз данных, SQL-инъекция, аудит безопасности, тестирование баз данных, малый бизнес, кибератаки.*

По данным «Ростелеком-Солар», которые компания опубликовала 20 февраля 2023 года, только в 2022 году число кибератак удвоилось и стало достигать 911 тыс.[[1]](#footnote-1)

Крупные корпорации, правительственные организации и финансовые структуры выделяют миллионы долларов на обеспечение информационной безопасности своих компаний, но они не могут справиться с традиционными атаками, большинство из которых можно предотвратить известными методами защиты информации.

Особенности предприятий малого бизнеса:

1. На первое место ставят продуктовую, операционную или маркетинговую деятельность, не считая приоритетной задачу разработки четких стратегий обеспечения защиты информации и развития IT-инфраструктуры.
2. Не обладают квалифицированным персоналом. Многие небольшие компании не имеют штатного специалиста по IT, поэтому об отдельном специалисте по ИБ даже и речи идти не может.

Существует лишь малое количество ресурсов и статей рассказывающих о действительно полезных методах обеспечения безопасности баз данных, которые могут быть применимы для предприятий малого бизнеса.

Перед обеспечением безопасности баз данных предприятия стоит ряд задач:

* защита информации от несанкционированного доступа (НСД);
* предотвращение уничтожения данных;
* защита от программных и аппаратных ошибок, сложностей с доступом к серверу.

Задачи решаются различными способами и методами, выбор средств обеспечения безопасности основывается на понимании угроз, направленных на содержимое БД.

Среди основных угроз выделяют:

* несанкционированное использование информации в БД;
* атаки с помощью вирусов, которые могут повлечь различные последствия;
* SQL-инъекции;
* технические проблемы, снижение производительности;
* ошибки, недоработки, несанкционированные возможности в программах, управляющих базами, и ином ПО[[2]](#footnote-2).

Достаточно универсальным и надежным методом защиты базы данных, является тестирование. Оно проводится для обнаружения любых слабых мест или уязвимостей в конфигурации безопасности базы данных и для уменьшения последствий любого нежелательного доступа к базе данных.

Выделяют несколько техник тестирования:

1. Тест на проникновение. Это умышленная атака на систему с целью поиска уязвимостей и дыр в безопасности, через которые злоумышленник может получить доступ ко всей системе, включая базу данных. Когда в системе обнаруживается слабая сторона, все угрозы немедленно устраняются и ослабляются.

2. Оценка рисков. Это процесс выполнения анализа рисков, который определяет уровень риска, связанный с типом существующей конфигурации безопасности базы данных и возможностью обнаружения уязвимостей.

3. Проверка SQL-инъекции. Это включает в себя приведение в порядок значений, вставляемых в базу данных.

4. Взлом пароля. Все компании, в особенности те, которые разрабатывают или используют финансовые приложения, должны убедиться, что их система управления базами данных имеет строгую политику паролей.

5. Аудит безопасности. Необходимо регулярно проводить аудит безопасности, чтобы оценить политику безопасности организации и выяснить, соблюдаются ли стандарты или нет.[[3]](#footnote-3)

Различные предприятия имеют свои собственные специфические стандарты безопасности, и как только эти стандарты установлены, от них уже нельзя отказаться. Несоблюдение любого из этих стандартов является серьезным нарушением.

Метод тестирования очень хорош для поддержания безопасности базы данных на должном уровне. Важно отметить, что этот метод может быть использован как компаниями с многомиллиардными бюджетами, так и очень маленькими предприятиям малого бизнеса.

Но все же многие компании не могут позволить себе этот метод. Для таких случаев существуют общие принципы управления безопасностью базы данных, придерживаясь которых, можно повысить уровень защиты:

* необходимо выбирать защищенный сервер или платформу баз данных, предлагающие собственные системы аудита и мониторинга;
* ограничение физического доступа к компьютерам, на которых находятся элементы БД;
* обеспечение наличия системы резервного копирования и восстановления базы после сбоев;
* ограничение числа пользователей с правами администратора;
* использование сложных или одноразовых паролей для административных учетных записей, разработка инструкции для штатных сотрудников по составлению сложных паролей;
* запрет на установку неодобренных приложений;
* использование антивирусов с последними обновлениями антивирусной базы для защиты систем от вредоносного ПО;
* ограничение использования съемных носителей (USB, CD, DVD);
* использование многофакторной аутентификации;
* изменение паролей по умолчанию для всего (устройств, приложений и др.), что используется в компании;[[4]](#footnote-4)

Компаниям не должны жалеть бюджета для обучения своих сотрудников, рассказывая им об основных правилах безопасной работы в сети и за компьютерами. Так же необходимо, хотя бы раз в месяц, доносить своим сотрудникам информацию о новых угрозах Компетентные работники — отличная база для обеспечения безопасности информационной безопасности системы компании. Малому бизнесу необходимо универсальное решение по разумной цене, простое в установке и управлении, позволяющее гибко настраивать использование ресурсов предприятия, а также обеспечивать комплексную защиту от всевозможных угроз.

**Список литературы**

1. «Ростелеком-Солар» Привилегия с подвохом: свыше 60% компаний сталкиваются с угрозами привилегированного доступа ежемесячно. // https://rt-solar.ru/events/news/3358/ (дата обращения 12.03.2023 г.).
2. Информационная безопасность баз данных. // https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-baz-dannykh/ (дата обращения 13.03.2023 г.).
3. Типы угроз для базы данных. // https://habr.com/ru/company/otus/blog/557296/ (13.03.2023 г.).
4. Рекомендации по информационной безопасности для малого и среднего бизнеса (SMB). // https://habr.com/ru/post/348892/ (дата обращения 13.03.2023 г.).

1. «Ростелеком-Солар» Привилегия с подвохом: свыше 60% компаний сталкиваются с угрозами привилегированного доступа ежемесячно. // https://rt-solar.ru/events/news/3358/ (дата обращения 12.03.2023 г.). [↑](#footnote-ref-1)
2. Информационная безопасность баз данных. //https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-baz-dannykh/ (дата обращения 12.03.2023 г.). [↑](#footnote-ref-2)
3. Типы угроз для базы данных. // https://habr.com/ru/company/otus/blog/557296/ (13.03.2023 г.). [↑](#footnote-ref-3)
4. Кириллов П. Рекомендации по информационной безопасности для малого и среднего бизнеса (SMB). // https://habr.com/ru/post/348892/ (дата обращения 13.03.2023 г.). [↑](#footnote-ref-4)