**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:*** *Ежегодно число кибератак на организации разных масштабов растет в 1,5 – 2 раза. Также уже давно стали обычными новостями такие инциденты информационной безопасности как: утечки информации о кредитных картах, кража персональных данных, программы-вымогатели, кража интеллектуальной собственности, нарушение конфиденциальности, отказ в обслуживании, публикация в открытый доступ баз данных. Предприятия малого бизнеса не готовы выделять многомиллионные бюджеты на обеспечение своей безопасности, поскольку обладают достаточно ограниченными денежными и людскими средствами. Поэтому многие предприниматели обязаны знать несколько методов обеспечения информационной безопасности баз данных, которые могут быть применимы в условиях ограниченных ресурсов. Некоторые из них рассмотрены в этой статье.*

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

Только в одном 2022 году число кибератак удвоилось и стало достигать 911 тыс. О таких данных «Ростелеком-Солар» рассказал 20 февраля 2023 года.[[1]](#footnote-1)

Крупные компании и предприятия большого бизнеса, правительственные организации и финансовые структуры выделяют многомиллионные бюджеты на обеспечение информационной безопасности своей компании, и все же не справляются с обычными атаками, большую часть которых можно было 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;
* вирусные атаки с различными последствиями;
* SQL-инъекции;
* технические проблемы, снижение производительности;
* ошибки, недоработки, несанкционированные возможности в программах, управляющих базами, и ином ПО[[2]](#footnote-2).

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

Выделяют несколько техник тестирования:

1. Тест на проникновение. Это преднамеренная атака на систему с целью найти уязвимости в системе безопасности, благодаря которым злоумышленник может получить доступ ко всей системе, включая базу данных. При нахождении слабой стороны в систему немедленно происходит устранение и ослабление любой угрозы.

2. Оценка рисков. Это процесс проведения оценки риска для определения уровня риска, связанного с типом внедренной конфигурации безопасности базы данных, и возможности обнаружения уязвимости.

3. Валидация SQL-внедрения. Это включает в себя приведение в порядок значений, которые вставляются в базу данных.

4. Взлом пароля. Любые компании, особенно те, которые разрабатывают или используют финансовые приложения, должны убедиться в том, что они установили строгую политику паролей для своей системы управления базами данных.

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

Существуют различные предприятия со своими особыми стандартами безопасности, и если эти стандарты установлены, то от них уже нельзя отказаться. Если кто-то не соблюдает какой-либо из этих стандартов, то это будет считаться серьезным нарушением.

Метод тестирования очень неплохо помогает поддерживать на должном уровне защищенность базы данных. Важно отметить, что данным методом могут пользоваться как компании с многомиллиардными бюджетами, так и совсем небольшие предприятия малого бизнеса.

Но все еще многие компании не могут себе позволить этот метод. Поэтому существуют общие принципы управления безопасностью баз данных, при соблюдении которых может быть повышен уровень зашиты:

* 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, а также 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 (устройства, приложения и др.), что используется в компании;[[4]](#footnote-4)

Компании должны не 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 о новых угрозах. Грамотные работники – отличная база для обеспечения безопасности информационной системы компании. Для небольших компаний нужно универсальное решение за разумную стоимость, простотой установки и управления, которое позволит гибко настроить использование ресурсов компании, а так же обеспечит комплексную защиту от всех типов угроз, чтобы вопросы информационной безопасности не отходили на задний план.

**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)