

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет» РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-1 «Защита информации»

ОТЧЁТ

# по практическому занятию №1

**по дисциплине «Безопасность систем баз данных»**

Студент: Кутьин З.

Шифр учебной группы:

БББО-05-20

Принял: Кунин Н.Т.

**П1. Параметры аутентификации для защиты БД паролем**

Теоретические вопросы:

1. **обобщенная структура системы баз данных. Каналы утечки данных в системе баз данных;**



1. **комплекс организационно-технических мер защиты базы данных**

1. Организационные меры защиты, обеспечивающие ограничение круга лиц, являющихся пользователями корпоративной информационной системы и имеющих доступ в помещения узлов обработки данных (ЦОД) и вспомогательных служб.

*Охрана, ограждение, оборона, пропускной режим, комендатура,…*

2. Процедурные меры защиты обеспечивают доступ к данным и их обработку только строго определенному кругу пользователей в

соответствии с их полномочиями (уровнями благонадежности) – идентификация пользователей и выдача им паролей.

*Идентификация и аутентификация пользователей, уровни благонадежности пользователей (прикладных процессов)*

3. Структурные меры защиты реализуются в ходе проектирования логической и физической структур базы данных путем

разработки соответствующих возможным каналам утечки механизмов защиты.

*Классификация по степеням конфиденциальности, многозначность, имитация,…*

4. Аппаратные средства защиты, представляющие собой дополнительные технические устройства, встраиваемые в элементы

информационной системы или сопрягаемые с ними через стандартные интерфейсы.

*HASP-ключи, генераторы шума, имитаторы обмена, ON-LINE-шифраторы,…*

5. Программные меры, реализуемые с помощью специальных программ безопасности, являющихся компонентами серверных и

клиентских приложений.

*Программное шифрование, хеширование, инкапсуляция, разграничение доступа, резервное копирование и аварийное восстановление,…*

1. **уровень благонадежности пользователя;**

Каждый пользователь СУБД характеризуется степенью благонадежности, которая также определяется меткой безопасности, присвоенной данному пользователю. Пользователь может получить доступ к данным, если степень его благонадежности удовлетворяет требованиям соответствующей метки безопасности. Более точно:

· уровень секретности пользователя должен быть не ниже уровня секретности данных;

· набор категорий, заданных в метке безопасности данных, должен целиком содержаться в метке безопасности пользователя;

· набор областей, заданных в метке безопасности пользователя, должен целиком содержаться в метке безопасности данных.

1. **степень конфиденциальности данных;**

****

1. **механизм защиты данных –** правило установки соответствия между шкалой уровней благонадежности пользователей и совокупностью степеней конфиденциальности данных
2. **виды атрибутивного доступа к данным;**

* Правило атрибутивной защиты данных:

Каждому субъекту обработки данных (пользователю/прикладному процессу) для каждого минимально возможного (атомарного, неделимого) объекта БД (таблицы, колонки, представления, индекса, курсора, функции, последовательности, сегмента отката, табличного пространства, сессии, …) называется отдельная привилегия для отдельного вида операции обработки: S – выборка, U – модификация, I – вставка, D – удаление, A – преобразование структуры объекта БД

1. **принципы наделения пользователей полномочиями;**

* Принцип наименьший привилегии и разделения обязанностей – данные должны быть тщательно распределены между исполнителями как по содержанию атрибутов, так и по набору средств их обработки (INSERT, UPDATE, DELETE, SELECT и другие возможные), особенно это касается совместно используемых данных
* Принцип предоставления наименьшего количества привилегий – каждому субъекту обработки данных должны выдаваться минимально необходимые права по обработке каждой порции данных, в идеале на каждую ячейку, на практике не каждый объект базы данных (таблицу, представление, индекс, последовательность, хранимую процедуру, функцию, триггер и т.п.)

1. **последовательность операций аутентификации пользователя. Что такое фактор аутентификации;**

Последовательность аутентификации:

* Распознавание (идентификация) пользователя (Кто я?)
* Удостоверение, что пользователь – это тот, за кого он себя выдает (Докажи, что это именно ты, а не кто-то другой)
* Определение привилегий легитимного пользователя (Какую роль ты будешь исполнять и что тебе)

Фактор аутентификации – устойчивое свойство или характеристика субъекта доступа с оригинальными значениями набора данных аутентификации.

1. **способы повышения эффективности фактора аутентификации.**
2. Применение средств шифрования информационного фактора (шифрование, хеширование паролей).
3. Ограничение периода действия многоразового пароля.
4. Расширение алфавита многоразового пароля.
5. Ограничение числа последовательных неудачных попыток аутентификации.
6. Использование одноразовых паролей.
7. Применение несимметричных парольных систем (электронная цифровая подпись, с публичным ключом шифрования).
8. Использование камуфляжа для средства физического управления доступом (маскировка токенов, имитация токенов в мультифункциональные устройства и тому подобное).
9. Маскировка и/или шифрование файла данных аутентификации.
10. Многофакторная аутентификация (последовательное использование разнородных факторов в разных сочетаниях).

Практические задачи:

1.1. Дано: алфавит пароля состоит из 20 символов, минимальная длина пароля 4 символа, нарушитель применяет для подбора пароля алгоритм полного перебора, проверяющий одну комбинацию за 1,1 сек. Рассчитать время вскрытия одного пароля АИС, обслуживающей 15 пользователей и управляемой одним администратором.

**Решение:**

1.2. Если разрешить в качестве алфавита пароля использовать все буквы русского и английского языка в обоих регистрах, цифры и знаки препинания (в том числе символ подчеркивания, процент, знак вычитания), допустить смену пароля не чаще, чем 1 раз в 9 месяцев, то какова будет защищенность базы данных при минимальной длине пароля в 7 символов?

**Решение:**

1.3. Дано: нарушитель может проверять одну комбинацию пароля за время 2,6 сек. В АСУ пароли могут изменяться не чаще, чем один раз в год, и содержат только символы русского алфавита. Выработать рекомендацию по длине пароля, гарантирующего защищенность базы данных не ниже, чем 0,95. Считать, что в году может быть только 365 дней.

**Решение:**

1.4. Дано: система идентификации пользователя позволяет применить 65 символов в качестве алфавита пароля, длиной не менее 9 символов. Время проверки одного пароля составляет 3,2 сек. Требуемая защищенность – 0,98. Выработать рекомендацию по периоду смены пароля пользователя.

**Решение:**

1.5. Дано: нарушитель может проверять одну комбинацию пароля за время 2,6 сек. В АИС пароли могут изменяться не чаще, чем один раз в год, и содержат только символы русского алфавита (прописные и строчные). Выработать рекомендацию по длине пароля, гарантирующего защищенность базы данных не ниже, чем 0,95. Считать, что в году может быть только 365 дней.

Решение

1.6. Дано: алфавит пароля состоит из строчных символов английского языка, минимальная длина пароля 8 символов, нарушитель применяет для подбора пароля алгоритм полного перебора, исполняемый на процессоре INTEL Core I9 10 поколения, выполняющий одну инструкцию за 0,0001 сек. Для проверки каждой комбинации пароля выполняется 9134 инструкции процессора. Рассчитать время вскрытия всех паролей АСУ, обслуживающей 24 пользователя и управляемой одним администратором.

**Решение:**

1.7. Нарушитель знает длину пароля – 9 символов. Он, используя алгоритм тотального перебора, вскрыл его за 234 дня, 7 часов, 12 мин и 33,6 сек. В его распоряжении была ЭВМ, исполняющая 1 инструкцию процессора за 10,6 мс, а на проверку одной комбинации пароля в алгоритме предусмотрено 9287 инструкций. Установить требование к надежности пароля (вероятность его вскрытия), если учесть, что нарушитель не должен успевать вскрыть его до его смены на новый.

1.8. Дано: Длина пароля 6 символов, алфавит состоит из английских букв с учетом регистра, защищенность базы данных от НСД должна составлять не менее 0,98. Применяется временная блокировка пароля при трех попытках указать неверный пароль на время 3 минуты. Нарушитель применяет алгоритм тотального перебора. Разработать требование по допустимой продолжительности действия пароля.