SIT TECH

Зачем защищать данные в базах данных

Конкретные кейсы

Наталия Едка | Директор ООО «ЭсАйТи Тех» | +375 29 634 47 46

Содержание

Кто мы такие

Несколько слов о SIT Tech и группе компаний МЕРАТЕХ

SIT Tech

- Белорусская команда экспертов в различных областях ИТ
- Технологический партнер для автоматизации и цифровизации бизнеса: от поставки ИТ-оборудования до работы с данными и бизнес-процессами
- Центр компетенций по мониторингу ИТ-инфраструктуры и ее компонентов
- Центр технической поддержки продуктов Oracle, Гарда Технологии и ZStack

Группа компаний МЕРАТЕХ

- VAD-дистрибьютор технологических продуктов и решений
- Производитель серверного и компьютерного оборудования – бренд BVK
- Регионы покрытия: штаб-квартира в Беларуси, филиалы в России, Литве, Армении, Грузии, Китае
- 200+ сотрудников в штате
- 50+ прямых контрактов с вендорами
- 15 000 SKU в портфеле

МЕРАТЕХ

Наши сертификаты

Развитие и подтверждение компетенций – неотъемлемая часть нашей работы

44	Oracle HW, SW, Administration, Implementation, Support
23	Oracle Presales/Sales
6	Гарда Технологии
2	Linux
6	ZStack
5	AppDynamics
3	Ivanti
2	Автоматизация БП

91
сертификат

Наши услуги

Обследование ИТ-инфраструктуры заказчика с выдачей рекомендаций по оптимизации и услуги по их применению

- Анализ сегмента ИТ-инфрастуктуры
- Анализ настроек СУБД и приведение в соответствие с лучшими бизнес-практиками вендора
- Оптимизация работы с реальными результатами по увеличению производительности, экономии места для хранения данных и т.п.
- Короткие сроки проекта, по результатам – подробный отчет с рекомендациями
- Приемлемые цены (бюджет до 1000 б.в.)

Услуги по сопровождению СУБД на всем жизненном цикле

- Создание и сопровождение хранилищ данных
- Миграция и модернизация СУБД
- Резервное копирование и восстановление СУБД
- Техническая поддержка 24x7 согласно SLA, полное соответствие требованиям заказчика

Наши услуги

Внедрение решений по информационной безопасности. Защита баз данных

- Предотвращение массовых утечек данных
- Предотвращение кражи конкретных данных
- Защита данных от изменений, удаления
- Маскирование данных перед передачей разработчикам, в тестовый контур

Создание корпоративных систем мониторинга

- Мониторинг ИТ-инфраструктуры, приложений, сервисов
- Мониторинг специализированных устройств: банкоматов (включая диспенсер, сбросовые кассеты, кассеты с денежными средствами, картридер и т.п.), кондиционеров, весов и любых других устройств, умеющих отдавать информацию о себе
- Визуализация важных для команды сопровождения показателей
- Настройка реакций системы мониторинга на события и оповещения ответственных администраторов
- Автоматизация процесса управления конфигурациями

Наши услуги

Платформа виртуализации

- Достойная альтернатива VMWare
- Сертифицированное в ОАЦ решение
- Поставка, внедрение, ТП 24x7 на русском языке
- Пилотные проекты, предоставление заказчику доступа к демо-стенду

Услуга по автоматизации бизнес-процессов (HelpDesk/ServiceDesk)

Поставка оборудования и ПО, интеграция с существующей инфраструктурой, ввод в эксплуатацию

- Разработка архитектуры ЦОД
- Поставка серверов, систем хранения данных, сетевого оборудования
- Пусконаладочные работы
- Гарантия до 5 лет
- Склад оборудования в Минске

Наши услуги

Техническая поддержка всего спектра поставляемых решений

- ТП 24x7, выполнение SLA
- Все доступные каналы регистрации инцидентов: собственный сервис-деск, email, мобильный телефон, мессенджеры
- Консультации по вопросам установки и настройки оборудования и ПО
- Решение инцидентов, предоставления ZIP на замену
- Выделенный эксперт
- Сертифицированные инженеры

Статистика хищения данных

Насколько надежно компании защищают данные?

30%
организаций столкнутся с утечкой данных в ближайшие 2 года

$3.86 млн
средняя стоимость утечек данных для организаций

191 день
среднее время обнаружения факта утечки данных

Число жертв кражи персональных данных в мире с 2004 г. вдвое превысило население Земли

- Число утечек = 14,9 млрд
- Число жителей планеты Земля – 7,95 млрд

Статистика утечки информации (SurfShark и purplesec.us/resources/cyber-security-statistics/)

Утечка данных в банках России

2023

В открытый доступ попали данные клиентов Альфа-банка (октябрь) – 1 млн. строк

Роскомнадзор подтвердил утечку данных 1 млн клиентов МТС-банка

В сеть попали данные 47 млн пользователей «СберСпасибо»

2022

Число утечек данных в российском финансовом секторе за 2022 год выросло на 71% в сравнении с 2021

70% утечек - по причине действий их сотрудников

В общей сложности из российского финансового сектора за 2022 год утекло около 44,8 млн записей персональных данных и платежной информации (рост в 32 раза в сравнении с 2021-м), из мирового – более 627 млн записей

Продажу данных 5,6 тыс. клиентов МТС Банка. Топ менеджер осужден на 3,5 года колонии строгого режима и выплате штрафа в размере свыше 5 млн рос. руб.

2021

За год слито 20 новых баз данных. 3 из 20 баз данных содержали более 100 тыс. записей о клиентах:

Информацию о 150 тыс. желающих взять кредиты в Совкомбанке

Примерно 100 тыс. — в банке «ДОМ.РФ»

Предложение о продаже данных 0,5 млн. клиентов «Сбербанк Премьер» (специальной программы Сбербанка для обслуживания постоянных клиентов на привилегированных условиях)

Источники: https://www.tadviser.ru/, InfoWatch

Утечка данных в Беларуси

2023

В конце марта на одном из белорусских предприятий произошел инцидент: из-за несанкционированного доступа к его информационным системам незаконно были распространены персональные данные 55 тыс. граждан

buslik.by – данные более 220 тыс. человек

«Остров чистоты и вкуса» – 730 тыс. человек

Фирма «Юркас» (поставки и производство дверей) – 5 тыс. клиентов фирмы

Сеть салонов цифровой техники «Алло» (ООО «ПАТИО плюс») – 16 тыс. человек

По данным МВД за 1-й кв. этого года возбуждено порядка 500 уголовных дел по фактам совершенных мошеннических действий в отношении граждан

2022

«Соседи» – более 630 тысяч записей ПД о клиентах

«Остров чистоты и вкуса» – более 140 тысяч

Оператор доставки еды «Just-eat» – более 230 тысяч,

Крупный банк – около 42 тыс.

Интернет-магазин nlstar.by – 85 тыс. клиентов

Источники: НЦЗПД, МВД

SIT TECH

ГАРДА

Защита данных в БД

DAM/DBF-система Гарда БД – Гарда Технологии

Гарда БД

Общие соображения

1. Защищаем не только саму СУБД, но и данные в ней
2. Прежде чем злоумышленник совершит хищение, он должен данные достать из БД . Гарда его точно увидит на уровне доступа
3. Важны не только запросы, но и ответы
4. Гарда защищает не только от утечек!

Помогут ли штатные средства защиты?

Спойлер: есть проблемы

Аудит доступа к данным СУБД входит во все мировые стандарты безопасности

Недостатки аудита средствами СУБД

- Нагрузка на аппаратную часть
- Сложность настройки
- Возможность отключения
- Сложность анализа
- Невозможность анализа ответа

Последствия

- Ограниченное количество правил аудита → вероятность «проглядеть» инцидент
- Отдаем настройки администратору → риск
- Вероятность проглядеть инцидент, пока аудит не работает
- Тратим время

6 групп кейсов – 6 типов решаемых задач

Основные кейсы

1. Массовая кража данных (слив базы)
2. Кража конкретных данных
3. Изменение данных
4. Кейсы, связанные с требованиями регуляторов
5. Кейсы, связанные с настройками БД
6. Косвенные признаки инцидентов

Массовая кража данных

Особенности кейсов

Что

- Персональные данные
- Номера банковских карт
- Дни рождения+ФИО / email+ФИО
- Номера скидочных карт
- Учетные данные
- Хэши паролей
- ФИО+телефон / ФИО + email
- Список клиентов/контрагентов

У кого

- Банки
- Телеком
- Кредитные организации
- Страховые компании
- Медицинские учреждения
- Ритейл
- Туроператоры

Утечка данных. Массовая выгрузка

Пример: Массовая кража через временную таблицу

Кейс	Массовая кража данных через временную таблицу
Кто	Подрядчик
Как	Подрядчик создает таблицу для технических нужд. Передает SQL-скрипт для выполнения администратором, где спрятана команда выгрузки данных во временную таблицы. Далее подрядчик выгружает временную таблицу себе в файл
Решение	Фиксирование создания нового объекта в БД Фиксирование выгрузки аномально большого количества записей во временную таблицу Запись в файл из временной таблицы

Утечка данных. Массовая выгрузка

Маскировка под легитимный процесс

Кейс	Массовая кража данных с маскировкой под легитимный процесс
Кто	Привилегированный пользователь
Как	Зная о запрете на большие выгрузки создается скрипт на выгрузку небольших пакетов данных из БД, который запускается с периодичностью раз в минуту
Решение	Профилирование поведения пользователя Фиксирование аномального отклонения в поведении

Утечка конкретных данных

Особенности кейсов: модель угроз, утечки через легитимный доступ, мониторинг БП

Банки

- Слив информации о поступлениях на банковский счет
- Слив информации о совершенных платежах
- «Пробивка» состояния счета, наличия дополнительных счетов, поиск забытых счетов (не обращались больше года)

КВОИ

- Координаты объектов КВОИ
- Учетные данные различных ИС
- Данные различных датчиков, любая информация для подготовки терактов (транспортные карты, расписание смен постов охраны и т.п.)

Телеком

- «Пробив» паспортных данных по номеру
- Просмотр чужих SMS-сообщений
- История местоположений
- Платежная информация

Промышленность

- Слив информации о составе участников торгов и предложениях
- Адреса поставщиков и закупочные цены
- Суммы контрактов

Ритейл

- Маркетинговые акции
- Поставщики
- Учетные данные Интернет-магазинов
- Платежная информация клиентов

Утечка данных. Конкретные данные

Примеры решаемых задач

Кейс	Поиск номера телефона для коллектора. Уточнение остатков на счетах
Кто	Привилегированный пользователь
Как	Пользователь имеет права на работу с таблицей в базе данных. Используя стороннее программное обеспечение узнает номера телефонов, сумму остатка на счете и передает данные коллекторам
Решение	Создание политики контроля обращения к конкретным данным Создание профилей пользователей для выявления аномалий в поведении Просмотр графических отчетов

Утечка данных. Конкретные данные

Примеры решаемых задач

Кейс	Слив данных о новых местоположении, состоянии, структуре защищаемых объектов
Кто	Привилегированный пользователь
Как	Пользователь запрашивает координаты местоположений критических объектов инфраструктуры
Решение	Создание политики контроля обращения к конкретным данным Создание профилей пользователей для выявления аномалий в поведении Просмотр графических отчетов Проведение расследований

Изменение данных в базе данных

Особенности кейсов

- Основной нарушитель – администратор БД
- Общий принцип: использование этапа временного хранения данных в процессе выполнения бизнес-функции
- Мошенничество совершается в сговоре
- Для настройки Гарда БД требуется глубокое понимание бизнес-процесса

Изменение данных в базе данных

Примеры решаемых задач

Кейс	Изменение страховой суммы или суммы кредита
Кто	Привилегированный пользователь
Как	Пользователь умышленно изменяет назначенную страховую сумму или одобренную сумму кредита по сговору
Решение	Создание политики контроля изменений данных Создание профилей пользователей для выявления аномалий в поведении Проведение расследований

Изменение данных в базе данных

Примеры решаемых задач

Кейс	Перевод остатков счетов на свой дебетовый счет. Открытие и закрытие счетов
Кто	Привилегированный пользователь
Как	Пользователь умышленно переводит остатки с «забытых» счетов и получает %. Или по сговору с криминальными структурами путем открытия и закрытия счетов выводит деньги
Решение	Создание политики контроля изменений данных Создание профилей пользователей для выявления аномалий в поведении Проведение расследований

Кейсы, связанные с настройками БД

Особенности кейсов

- Изменение конфигурационных файлов
- Смена паролей и технологических учетных записей
- Изменение настроек безопасности:
  - изменение уровня логирования
  - ограничение на число неудачных попыток входа
  - включение небезопасных параметров (удаленная идентификация средствами ОС)
  - Разрешение на запуск небезопасных процедур, выполняющихся от УЗ администратора
- Изменение роли учетной записи
- Добавление новых хранимых процедур

Изменение конфигурации базы данных

Примеры решаемых задач

Кейс	Включение параметра удаленной идентификации средствами ОС
Кто	Привилегированный пользователь
Как	Привилегированный пользователь меняет конфигурацию базы данных для открытия возможности доступа в БД и слива данных под неконтролируемой учетной записью
Решение	Сканирование на уязвимости Создание профилей пользователей для выявления аномалий в поведении Проведение расследований

Косвенные признаки инцидентов

Гарда БД

- Не всегда событие в СУБД однозначно свидетельствует об инциденте
- Подозрительные запросы надо ставить на контроль и отправлять в SIEM для корреляции с другими событиями других СЗИ
- В ГБД есть рекомендуемый перечень событий, подлежащий контролю (смены пароля, изменение прав, создание хранимой процедуры и др.
- Создавать отдельные политики по мониторингу:
  - Действий администраторов
  - Действий технологических УЗ (встроенных в СУБД)
  - Обращение к таблицам с ПДн или другой критической информации (по тексту ответа)

SIT TECH

ГАРДА

Обезличивание данных

Гарда Маскирование

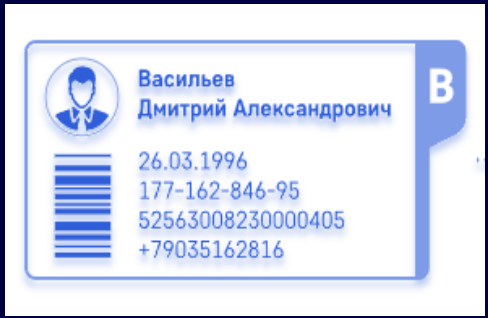
Как происходит обезличивание?

1 этап: Сканирование

- Автоматический анализ структуры базы данных
- Выявление персональных данных и другой конфиденциальной информации
- Настройка параметров маскирования

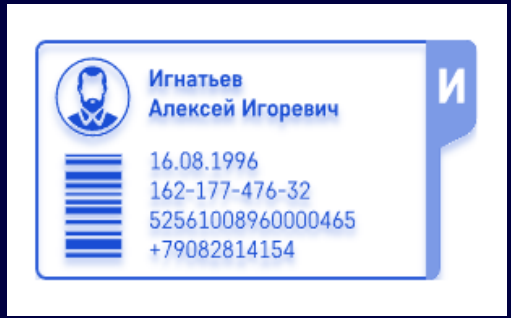
2 этап: Перенос данных

- Создание копии БД
- Замена персональных данных и другой конфиденциальной информации (обезличивание)
- Сохранение взаимосвязей, форматов и структур данных
- Формирование результирующего отчета



Поддерживаемые СУБД
Oracle | MySQL
PostgreSQL | MSSQL

Методы обезличивания
Генератор ФИО
Генератор номеров карт
Перемешивание
Случайная строка



SIT TECH

ГАРДА

Почему мы выбрали Гарда Технологии

Гарда БД Гарда Маскирование

Почему мы выбрали Гарда Технологии

- Наличие сертификатов ОАЦ: Гарда БД | Гарда Маскирование | Гарда Предприятие
- Поддержка большого количества СУБД – более 30 (ГАРДА БД)
- Бесплатные пилотные проекты
- Доработка функционала по требованиям заказчиков

150+

внедрений во всех отраслях

16 лет

опыта разработки систем высокой сложности

250+

высоко-квалифицированных сотрудников

5

запатентованных технологий собственного исследовательского центра

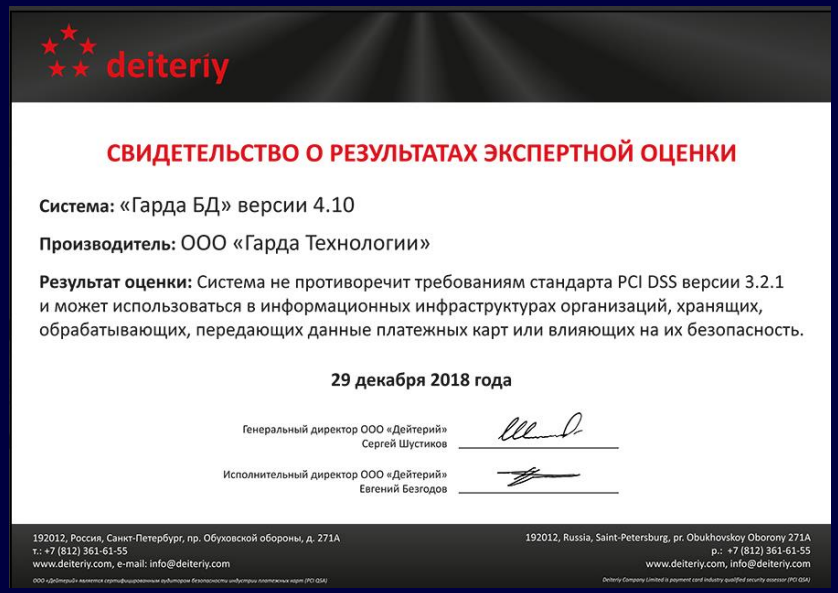
Соответствие требованиям регуляторов

Гарда БД

- Закон Республики Беларусь «О защите персональных данных» от 07.05.2021 №99-З
- GDPR (Европейский регламент по защите персональных данных)
- PCI DSS (Международный стандарт безопасности данных платежных систем)

Сертификация

Сертификаты решений компании Гарда Технологии



SIT TECH

Почему нас выбирают

SIT Tech – золотой партнер Гарда

Центр компетенций по продуктам Гарда

Комплексный подход к защите данных

Основные задачи

- Обеспечение физической целостности
- Обеспечение логической целостности
- Исключение несанкционированного доступа
- Исключение несанкционированного изменения/копирования
- Обеспечение доступности для «законных» пользователей

Пилотные проекты до принятия решения о приобретении

Как начать пилотный проект по защите или обезличиванию данных

Шаг 1	Заполнить опросные листы
Шаг 2	Получить техническое решение и план пилотного проекта
Шаг 3	Подготовить инфраструктуру /получить от нашей компании необходимое оборудование для проведения пилотного проекта
Шаг 4	Участвовать в пилоте и изучить функциональные возможности выбранного решения в условиях вашей ИТ-инфраструктуры
Шаг 5	Получить отчет о ходе пилотного проекта и рекомендации по дальнейшему внедрению и использованию программного продукта в вашей ИТ-инфраструктуре

В завершение

- Пользователь, прочитав и подписав согласие на обработку ПДн, перекладывает всю ответственность на Оператора ПДн (согласно закону №99-З).
- Организация-Оператор несет всю ответственность за сохранность и целостность ПДн.
- Мы призываем не экономить на ресурсах и средствах для обеспечении безопасности данных ваших клиентов.
  Это ваша репутация и ваш спокойный сон!

Приглашаем на наш стенд!

SIT TECH

Команда экспертов ООО «ЭсАйТи Тех»

+375 17 355 09 61 доб. 265

info@sit-tech.by

220138, г. Минск, пер. Липковский, 12-225