



Обзор функционала Protegrity

**Единственный путь
защиты важных данных
– это хранение данных
в защищенной форме**

Как мы защищаем данные?

В покое

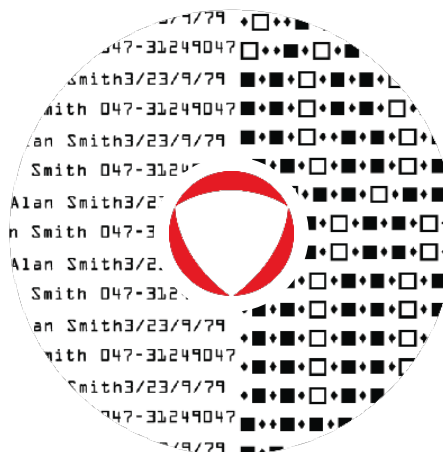
В пути

В эксплуатации

Данные, как центр безопасности



**Мы защищаем
данные на каждой
платформе и
устройстве на
предприятии и в
облаке**



**Защищенное
хранение данных,
как лучшее решение
для их безопасности**



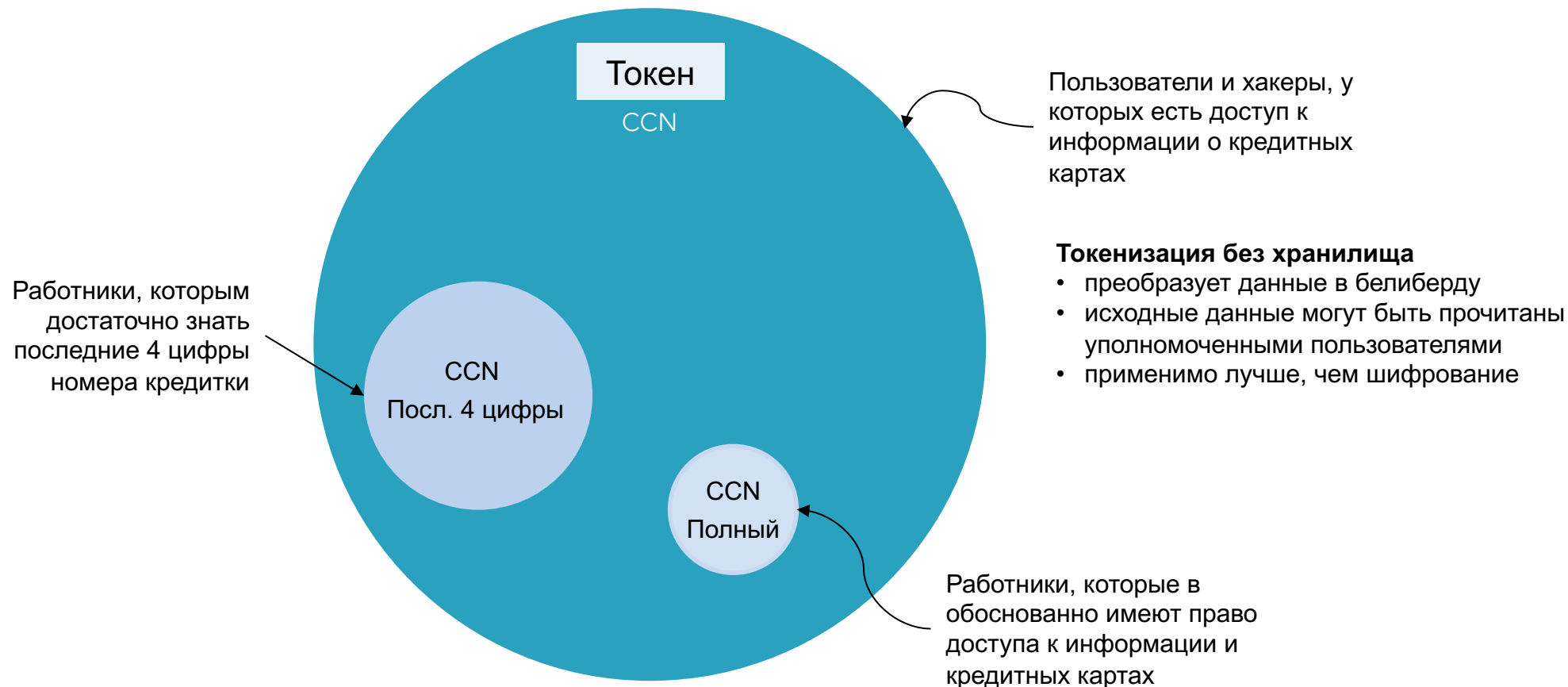
**Единый кросс-
платформенный набор
политик безопасности
для всех устройств**

Как можно защитить ценные данные?

- Методы защиты и де-идентификации данных:
 - Необратимое замещение путем редактирования
 - Необратимое хэширование
 - Обратимое шифрование (AES)
 - Обратимая токенизация (замещение данных на основе теории случайных чисел без сохранения пар соответствия)

Персональные данные / Данные здравоохранения							Можно не защищать
Имя	Адрес	Дата рождения	Номер паспорта	Номер кредитной карты	Адрес электронной почты	Номер телефона	Заметки
Иван Грозный	1 Палаты, Москва	25/02/1841	07674277841	3678 2289 3907 3378	prince@moscow.ru	492-00-8000	Данные, не относящиеся к чувствительным

Уменьшите риск и угрозу утечки данных



Granularity of Protecting Sensitive Data

Крупнозернист

ая защита
(файлы и тома)



- Методы: шифрование файлов и томов
- "Всё или ничего"
- Не защищает во время использования
- Шифрование на уровне ФС
- Шифрование HDFS
- Защита данных в покое и в пути

Мелкозерниста

я защита
(поля данных)

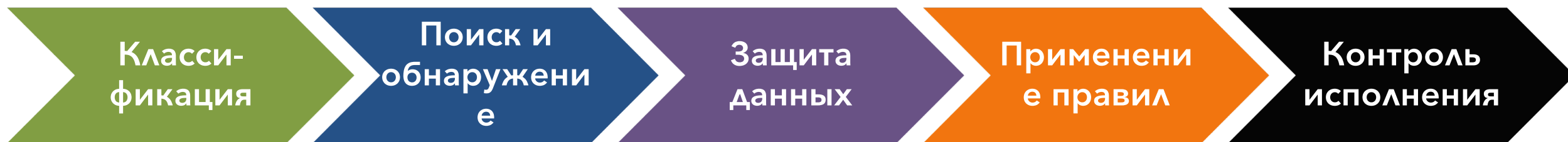


- На уровне полей
- Методы:
 - Токенизация без хранилища
 - Хэширование
 - Шифрование (AES, FPE с AES)
- Данные защищены независимо от места хранения
- Сохранение рабочих процессов

Мелкозернистая защита данных

Поле	Нешифрованный вид
Имя	Иван Грозный
Адрес	1 Палаты, Москва
Дата рождения	25/02/1841
Номер паспорта	07674277841
Номер кредитки	3678 2289 3907 3378
Почта	prince@moscow.ru
Номер телефона	492-00-8000

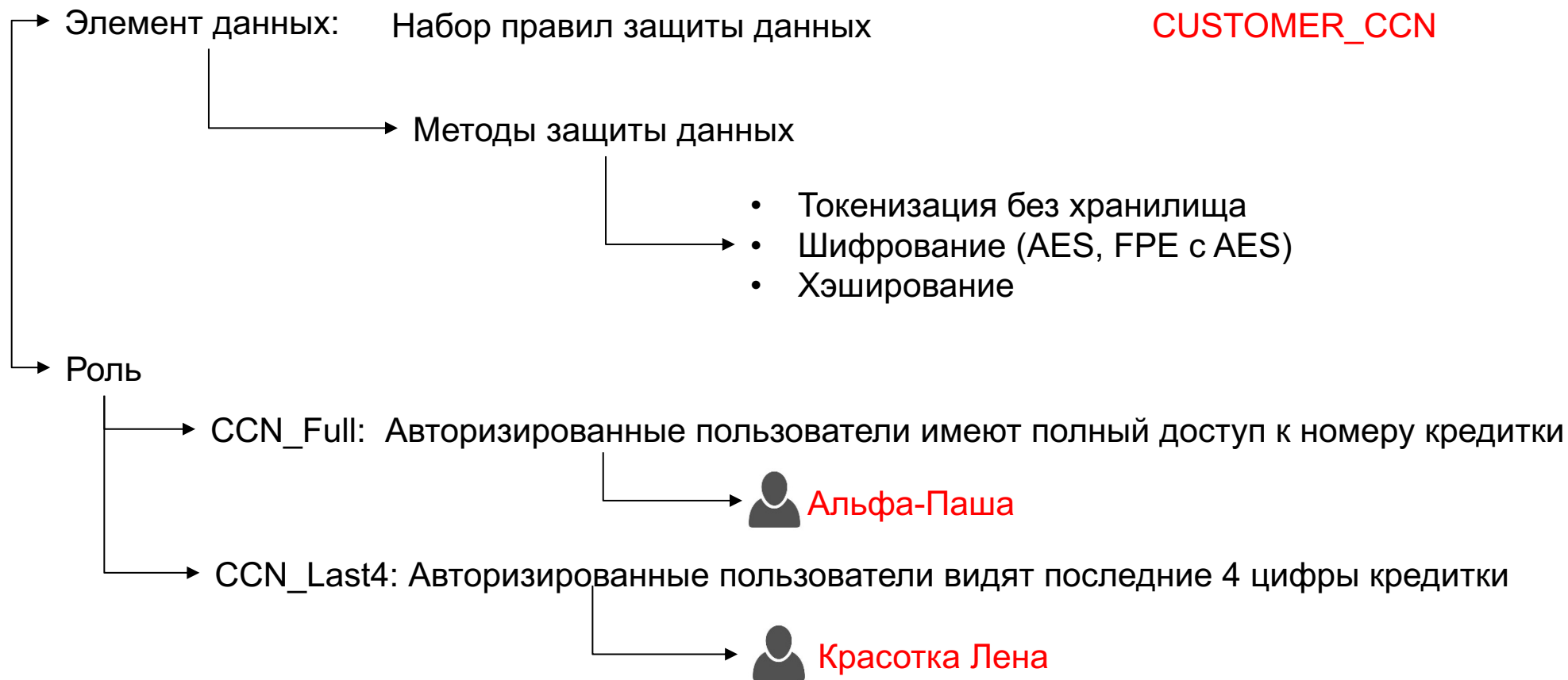
Обзор шагов



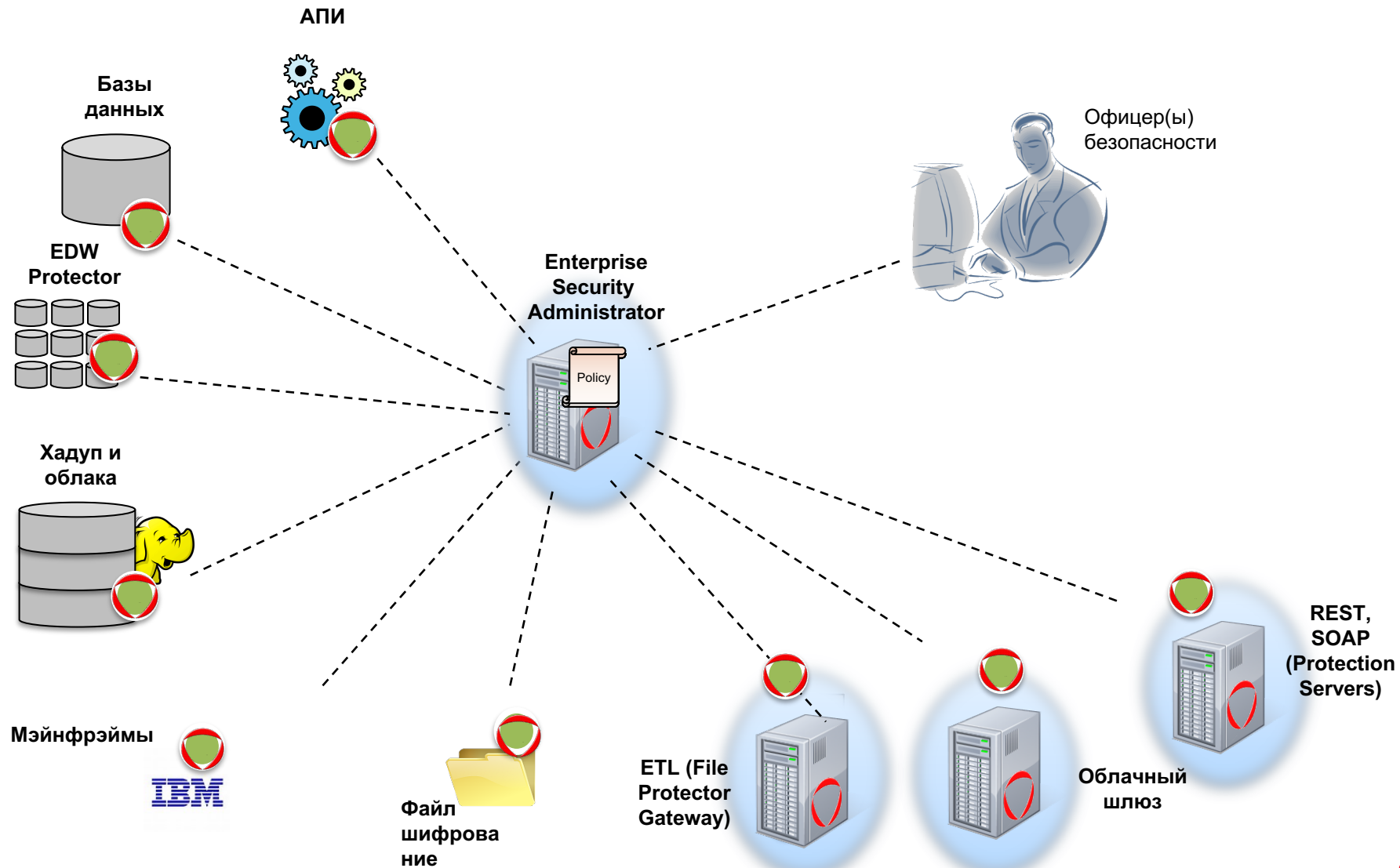
Политика защиты данных



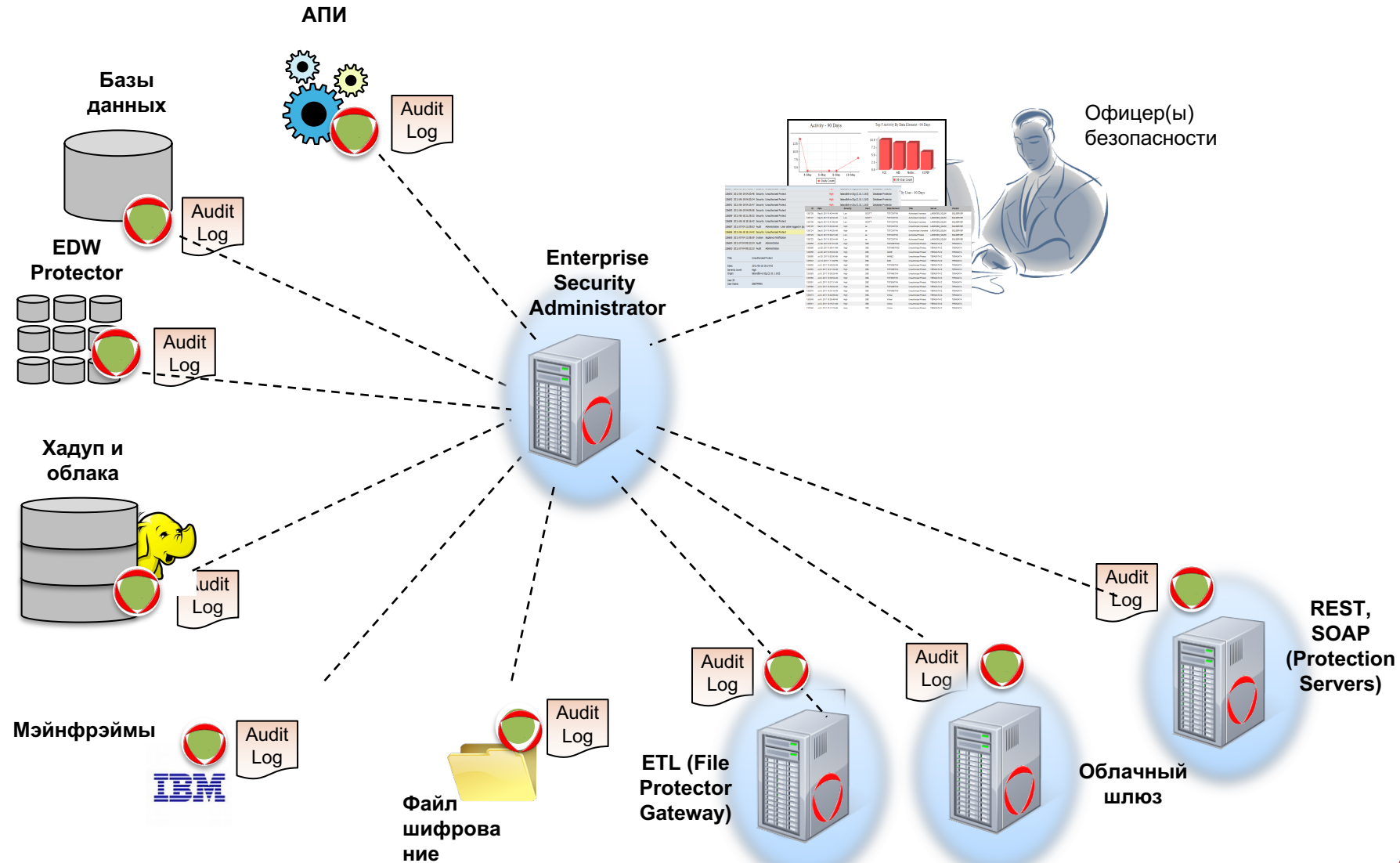
Политика защиты данных хранит правила и уровни доступа.



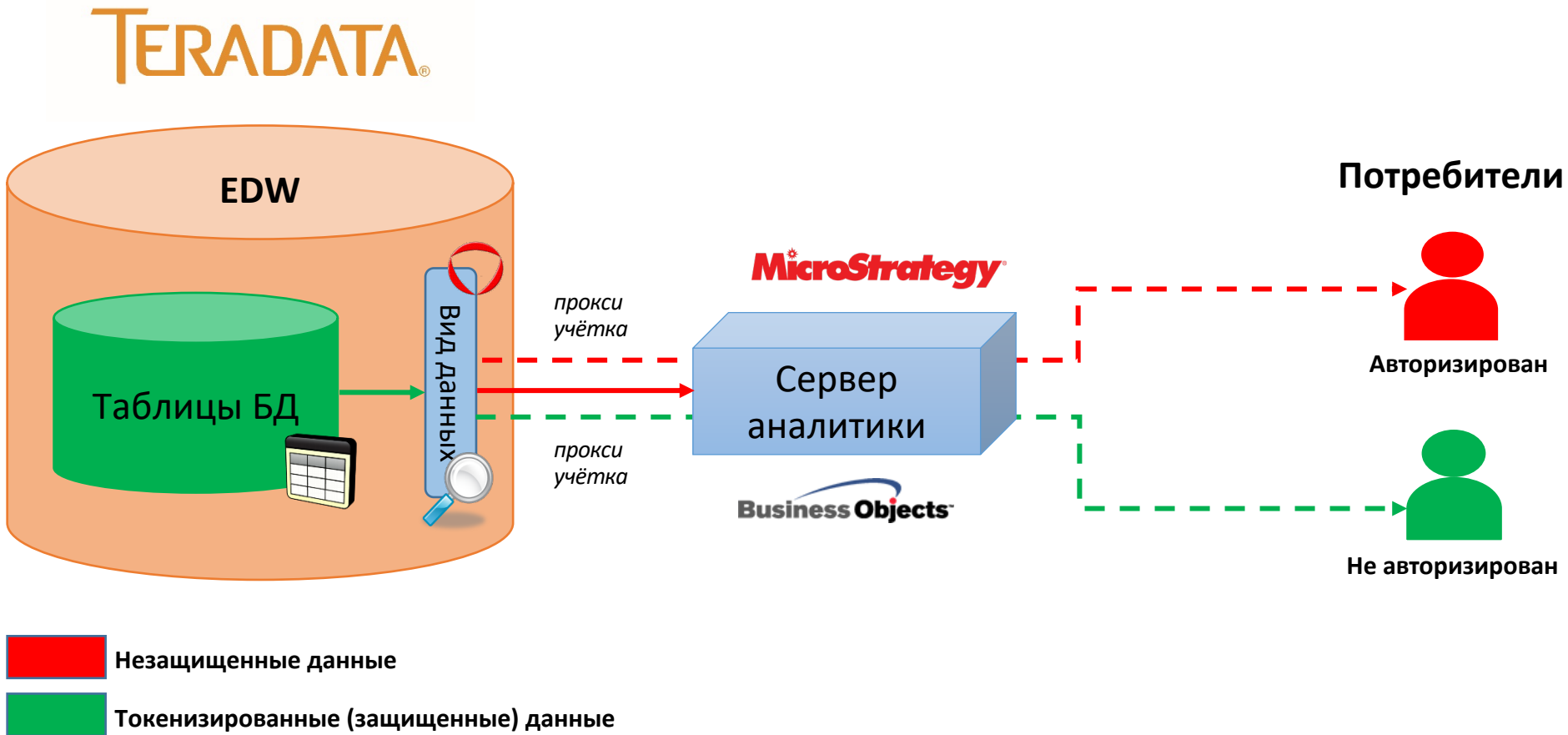
Централизованное управление – Развёртывание политики



Централизованное управление – Сбор журналов аудита

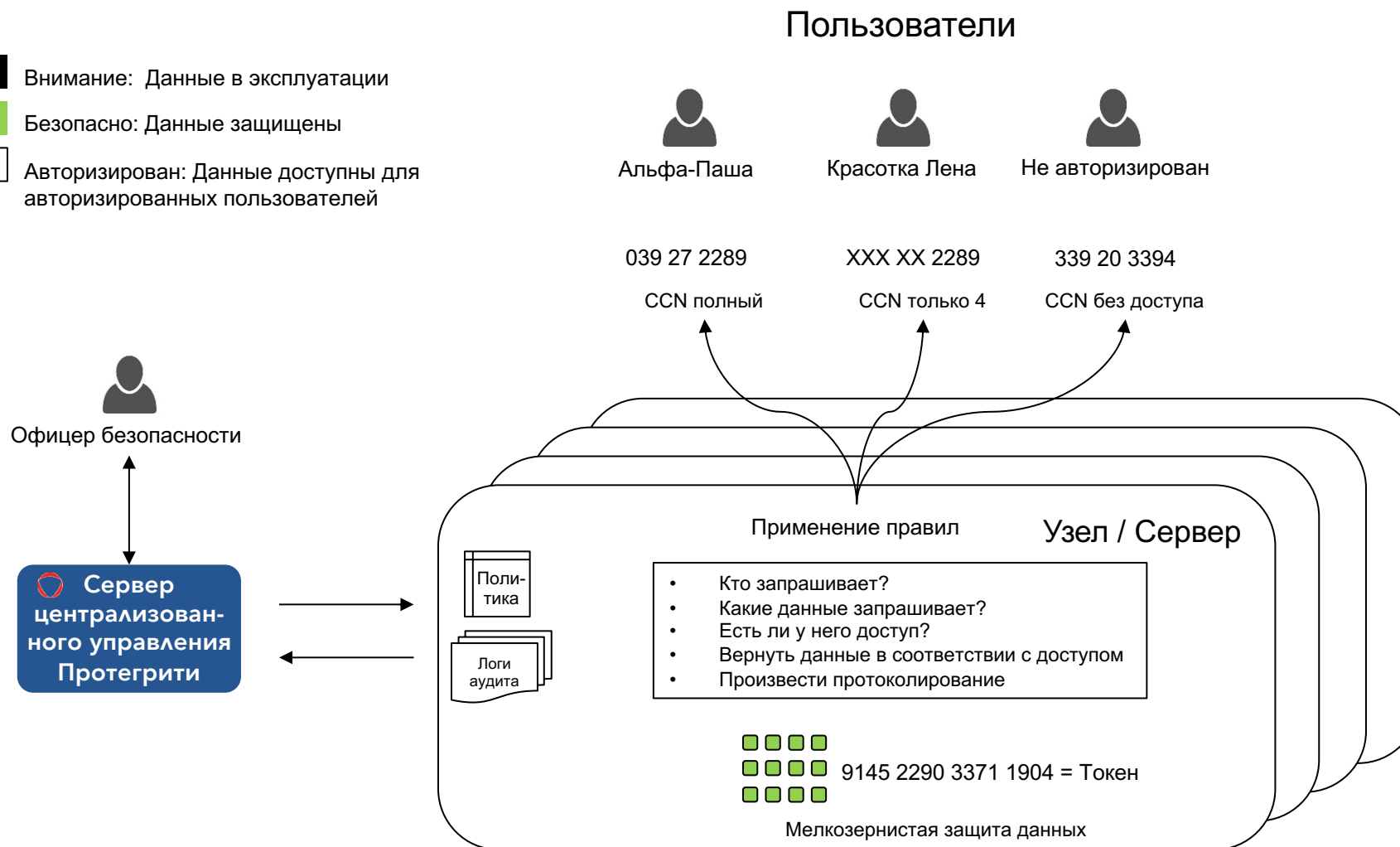


Конечные пользователи – Пример работы аналитики

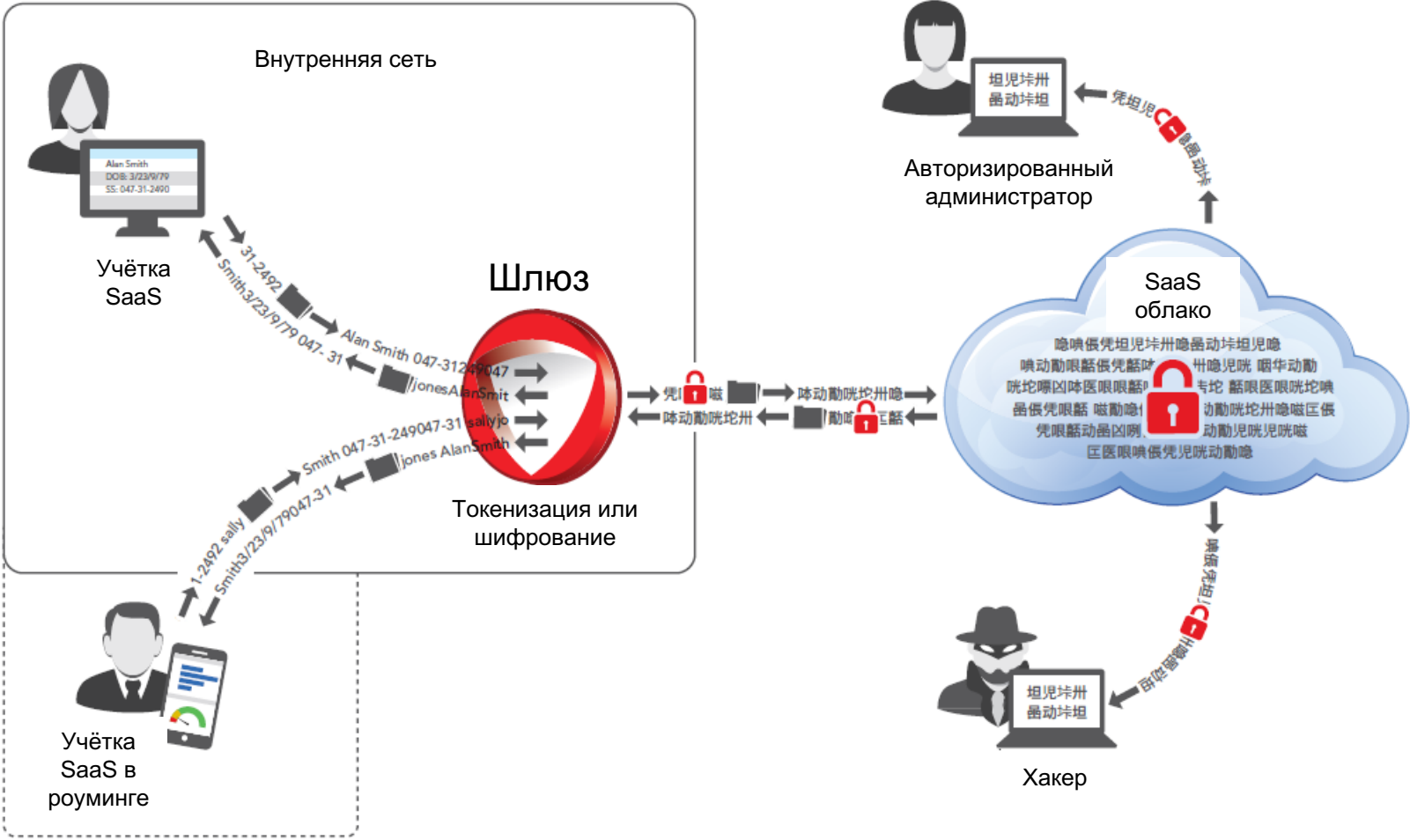


Применение правил доступа

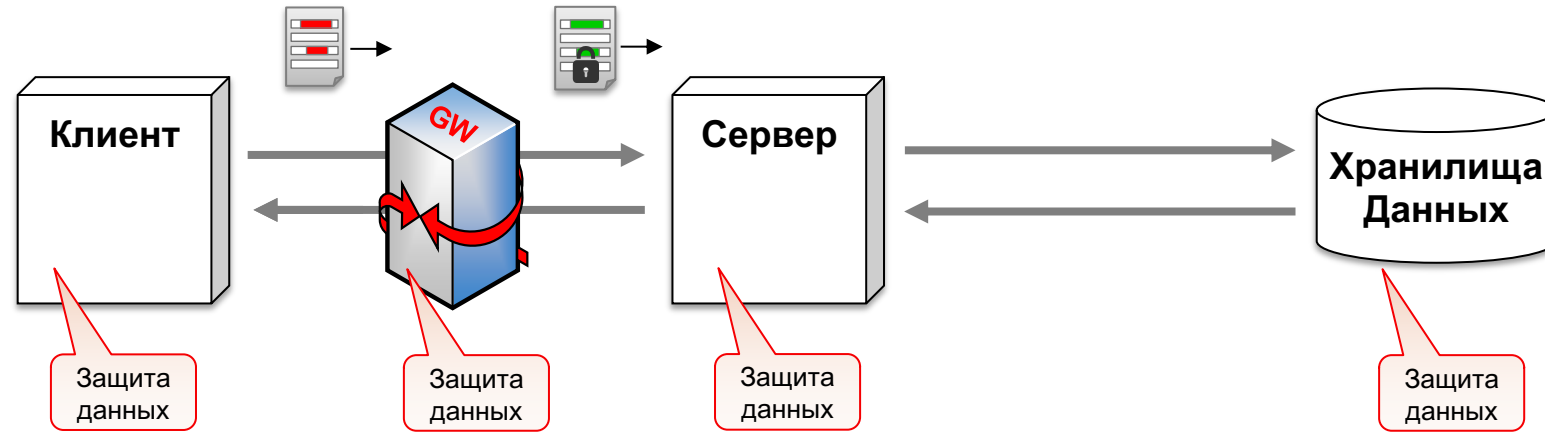
- Внимание: Данные в эксплуатации
- Безопасно: Данные защищены
- Авторизован: Данные доступны для авторизованных пользователей



Облачный шлюз Протегрیتی



Новый механизм защиты данных в потоке...



В поток данных между клиентом и сервером встраивается шлюз защиты данных. Ни сервер ни клиент не требуют какой-либо настройки. Шлюз выполняет следующие функции:

- Перехватывает стандартные и кастомизированные протоколы TCP/IP уровня приложения (например HTTP, SMTP, SFTP, SSH)
- Сканирует полезную нагрузку протокола (XML, HTML, JS, JSON, DOC(X), PPT(X), XLS(X), TXT, CSV, ZIP, PDF) на наличие конфиденциальных данных (посредством использования REGEX, XPath, JsonPath и т.д.)
- Преобразовывает данные защищенные<->незащищенные прямо в потоке.



Терадата и Протегрити

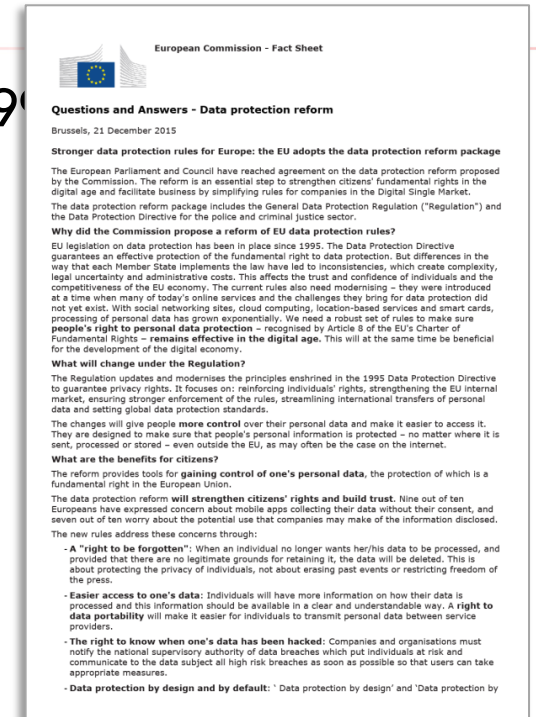
- Успешное стратегическое партнёрство с 2004 года
- Совместные исследования и разработки
- Решения Протегрити высокоинтегрированы, оптимизированы и сертифицированы для всего семейства продуктов Терадата
 - Teradata, Aster, Hadoop, облачные сервисы, DwaaS сервисы, хостинг приложений
 - Токенизация, шифрование, хэширование, маскирование и мониторинг
- Легко интегрируемое, масштабируемое и высокопроизводительное решение для Терадата
- Более 60+ общих клиентов по всему миру
- Ряд великолепных специалистов в Центре Экспертов Информационной Безопасности Терадата (InfoSec COE), как помощь во внедрении
- Чаще всего для защиты данных Клиенты Терадата выбирают Протегрити

Наши сильные стороны

- Независимый контроль доступа и журналирование
- Шлюз безопасности данных (DSG)
- Наивысшая гибкость в методах защиты данных
- Самая широкая родная поддержка множества платформ
- Самая широкая косвенная поддержка платформ посредством шлюза безопасности данных (DSG)
- Запатентованная, безопасная, PCI-DSS совместимая токенизация
- Крупно- и мелкозернистая защита данных от лидеров рынка

Общеввропейская Директива Защиты Данных (GDPR)

- Обновляет и дополняет директиву EU Data Protection Directive 1995
- Больше контроля и защиты для населения
- Основные положения:
 - 'Право на забвение'
 - Облегченный доступ населения к своим данным
 - Право данных на свободу перемещений
 - Уведомление властей в случае нарушений безопасности
 - Защита данных по умолчанию и в дизайне
 - Большие штрафы за несоблюдение правил (до 4% от оборота по всему миру)
- Директива поддерживает:
 - Анонимизацию
 - Псевдоанонимизацию (токенизацию)
 - Шифрование



**Единственный путь
защиты важных данных
– это хранение данных
в защищенной форме**

Десонстрация Протегрити

- ESA
- Защита для БД Терадата
- Защита для Hadoop Big Data
- Трансформации данных с ETL (FPG)
- Облачный шлюз

Токенизация без сохранения пар соответствия

Случайные, перемешанные, статические таблицы поиска



Токенизация Протегрити: Множество поиска

Номер кредитной карты

3845 9802 4484 7126

2791 **4393** 8350 7861

0000	9378
0001	6625
0002	2673
⋮	⋮
3844	8290
3845	7483
3846	5591
⋮	⋮
8398	8500
⋮	⋮
9999	4592

Токен

Токенизация без хранилища: Построение токена

Номер кредитки

3 8 4 5 9 8 3 0 2 9 8 4 7 1 2 6

Токен

7 4 6 2

случайно

Блок токена,
полученный из
таблицы,
случаен.

7462

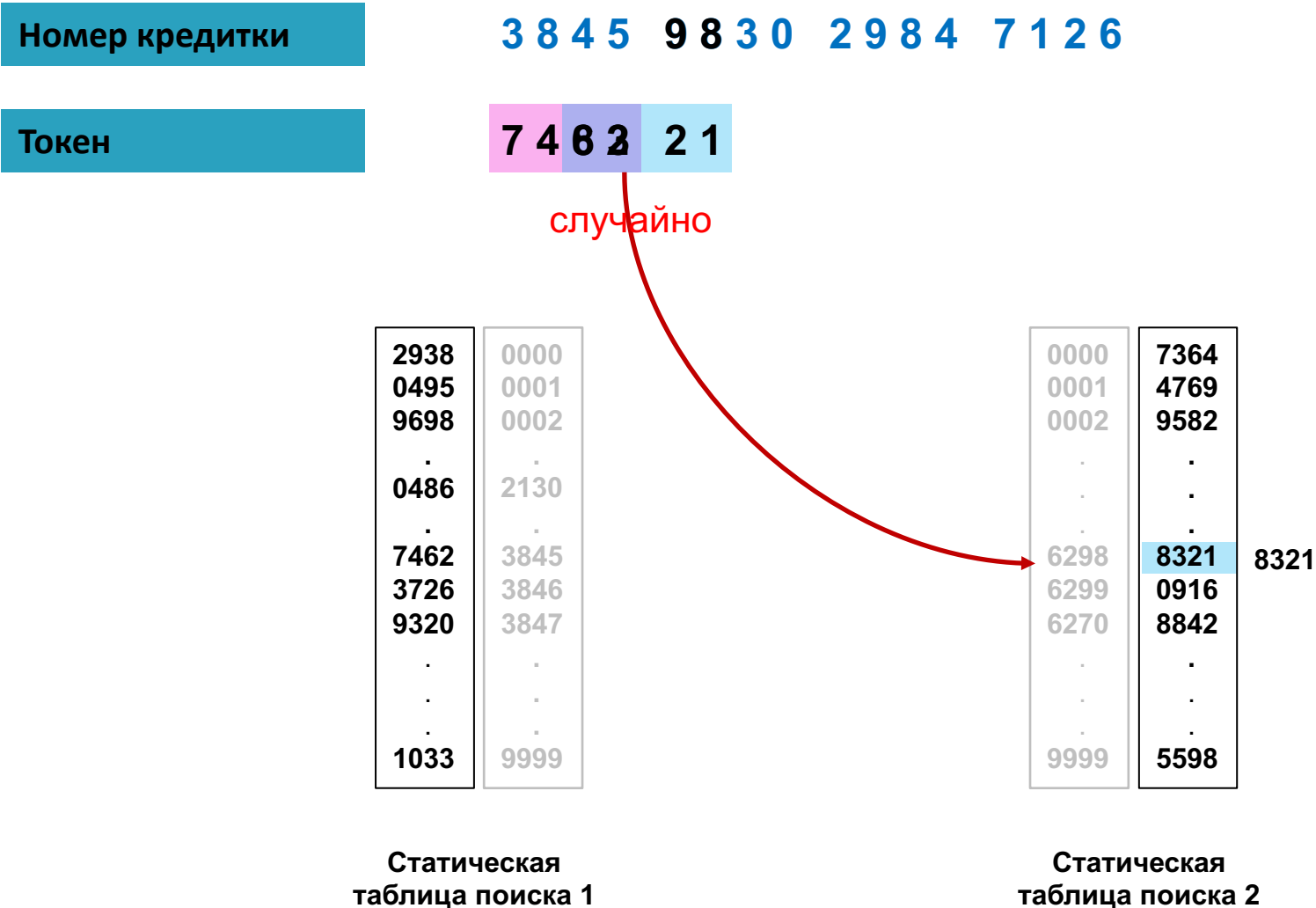
2938	0000
0495	0001
9698	0002
.	.
0486	2130
.	.
7462	3845
3726	3846
9320	3847
.	.
.	.
.	.
1033	9999

Статическая
таблица поиска 1

0000	7364
0001	4769
0002	9582
.	.
.	.
.	.
6298	8321
6299	0916
6270	8842
.	.
.	.
.	.
9999	5598

Статическая
таблица поиска 2

Токенизация без хранилища: Построение токена



Токенизация без хранилища: Построение токена

Номер кредитки

3 8 4 5 9 8 3 0 2 9 8 4 7 1 2 6

Токен

7 4 8 3 0 4 8 6 3 3 5 9 4 8 5 2

случайно

	2938	0000
	0495	0001
	9698	0002
	.	.
0486	0486	2130
	.	.
	7462	3845
	3726	3846
	9320	3847
	.	.
	.	.
	.	.
	1033	9999

Статическая
таблица поиска 1

Токен, полученный
путем подмены
блоков из
нескольких таблиц,
случаен.

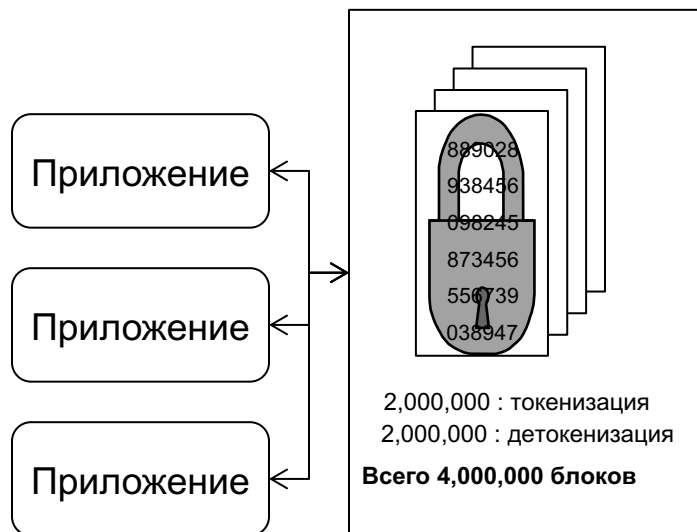
Проход слева на
право и обратно,
это один раунд.

Каждая
токенизация
требует 3 раунда.

0000	7364
0001	4769
0002	9582
.	.
.	.
.	.
6298	8321
6299	0916
6270	8842
.	.
.	.
.	.
9999	5598

Статическая
таблица поиска 2

Токенизация Протегрити



Потребляемая память:

3 символа $\approx$ 11.3 тысяч битов

6 символов $\approx$ 33.5 миллионов битов

Блоки токенов

- Статичны: остаются того же размера, что и в начале, независимо от количества сгенерированных токенов.
- Сгенерированы заранее: мгновенно готовы к работе.
- Лёгкие и маленькие: требуется всего 4,000,000 блоков для токенизации и детокенизации
- Таблицы содержат только блоки для токенизации и детокенизации, а не данные.
- Защищены: таблицы поиска зашифрованы.

Используемые технологии

- Случайное перемешивание по рекомендациям Петера Гуттмана с использованием Cryptlib (библиотека с исходным кодом и лицензией GPL)
- Шифрование AES-256 (библиотека OpenSSL)
- TLSv1.2 - SSL 3.0 (библиотека OpenSSL)