# Использование решений Oracle для обеспечения безопасности в соответствии с Общим регламентом по защите данных (GDPR)

ТЕХНИЧЕСКАЯ ПУБЛИКАЦИЯ ORACLE | ИЮЛЬ 2017

## Заявление об ограничении ответственности

Цель этой публикации — объяснить, как организации могут использовать решения Oracle для обеспечения безопасности в соответствии с определенными требованиями Общего регламента по защите данных (GDPR), принятого ЕС. Необходимость применения решений, описанных в этом документе, зависит от инфраструктуры или потребностей конкретной организации. Корпорация Oracle рекомендует всегда выполнять тестирование решений в среде их будущего применения, чтобы гарантировать должный уровень производительности, доступности и интеграции.

Информация, содержащаяся в документе, не является юридической рекомендацией в отношении содержания, интерпретации или применения законов, нормативных положений или директив и не может быть использована в этом качестве. Существующие и будущие клиенты Oracle должны самостоятельно обращаться за юридической консультацией в том, что касается применимости законов и нормативных положений к процессу обработки персональных данных, действующему в их компании, включая использование продуктов и услуг поставщиков.

## Введение

Многие организации пытаются оценить последствия принятия Европейским союзом нового Общего регламента по защите данных (GDPR), которые включают следующее.

- Потенциальные штрафы в размере до 4% от годового оборота, а также расходы на судебные издержки и услуги юристов.
- Пересмотр процессов, приложений и систем организации и внесение изменений.
- Обеспечение соответствия новым, более строгим требованиям к конфиденциальности и безопасности.

Приведение деятельности организации в соответствие GDPR требует скоординированной стратегии, затрагивающей юридический, кадровый, маркетинговый отделы, службы ИТ и безопасности и др. Действие GDPR может распространяться в том числе на информацию, получаемую из различных источников (например, от клиентов и сотрудников), а также средства связи и используемые технологии.

Организации должны разработать четкую стратегию и план действий и обеспечить соответствие требованиям GDPR не позднее 25 мая 2018 г.

Мы предлагаем нашим клиентам воспользоваться многолетним опытом и технологическими возможностями Oracle, чтобы соблюсти требования к безопасности. В этом документе рассказывается, как использовать решения Oracle для создания платформы безопасности в соответствии с требованиями GDPR.

## Разработка единой стратегии безопасности для предотвращения угроз, снижения рисков и обеспечения нормативно-правового соответствия

GDPR, скорее всего, является не единственным нормативным документом, требования которого вашей компании приходится соблюдать. Деятельность организации, как правило, регулируют множество законов и положений, а также глобальных отраслевых стандартов, которые направлены на защиту граждан, экономики, правительства и промышленности. Поэтому так важно иметь общую стратегию, которую можно было бы легко адаптировать в соответствии с изменениями в нормативно-правовых предписаниях.

Ужесточение требований к защите данных и конфиденциальности отчасти объясняется ростом числа краж данных и нарушений кибербезопасности. Неверно спроектированные с точки зрения безопасности ИТ-системы позволяют преступникам извлекать противозаконную выгоду, идет ли речь о шпионаже, организованной преступности или инсайдерских угрозах. Это в конечном результате препятствует свободному обмену информацией, который является одним из ключевых факторов для развития экономики и общества.

Для создания оптимальной стратегии по обеспечению нормативно-правового соответствия и снижению рисков организациям необходима глобальная платформа, которая включает в себя современные международные отраслевые практики, например, семейство стандартов ISO 27000 и др.

GDPR ставит своей целью использование передового опыта и надежных методов защиты. Согласно ему «контролеры» (например, компании, заключившие договор с поставщиком облачных услуг на обработку данных) и «обработчики данных» (например, поставщики облачных услуг) должны принять меры по обеспечению уровня безопасности, соответствующего тому риску, которому подвергаются права и свободы лиц («субъекты данных»), чьи данные собирает и использует контролер. Кроме того,

организация должна провести анализ рисков и принять необходимые меры (внедрить средства обеспечения безопасности) для противодействия этим рискам.

GDPR направлен на соблюдение ключевых принципов обеспечения конфиденциальности, целостности и доступности систем и данных. Компания Oracle давно и успешно занимается защитой данных и систем. Наши предложения включают в себя полный набор решений для гибридного облака, от интегральных схем до приложений, которые помогают прогнозировать, отслеживать и предотвращать угрозы безопасности и реагировать на них. Эти решения также позволят соблюсти требования GDPR.

Стратегически, внедрение подходящих технологий и эффективных средств обеспечения безопасности дает следующие преимущества.

- Соблюдение нормативно-правовых требований.
- Сокращение рисков (в соответствие с нормативными требованиями или для других целей).
- Повышение конкурентоспособности благодаря увеличению гибкости и сокращению времени выхода на рынок.
- Ускорение цифровой трансформации.

Кроме того, внедрение эффективной системы безопасности позволяет улучшить ИТ безопасность и ее организацию на предприятии.

## Основные положения GDPR о безопасности ИТ

GDPR включает в себя 99 статей и 173 пункта преамбулы и содержит важные требования к организации безопасности корпоративных систем ИТ.

Его основополагающим принципом является защита прав лиц, чьи данные собирают и обрабатывают организации, и эти права должны учитываться при разработке систем безопасности ИТ. В современном обществе системы ИТ используются повсеместно, и регламент требует, чтобы была обеспечена их безопасность.

В частности, для защиты персональных данных необходимо выполнить следующие действия.

- Выяснить, где хранятся данные (инвентаризация данных).
- Оценить степень риска (информированность о рисках).
- Провести проверку существующих приложений и при необходимости внести изменения (изменение приложений).
- Интегрировать средства обеспечения безопасности в архитектуру ИТ (интеграция в архитектуру).

Следующая таблица содержит наиболее важные статьи регламента, имеющие отношение к информационной безопасности.

КАТЕГОРИИ БЕЗОПАСНОСТИ ИТ И СТАТЬИ GDPR

| Категория безопасности ИТ | Статья GDPR |
|---|---|
| Инвентаризация данных | » *Ст. 30 «Журнал обработки»* |
| Информированность о рисках | » *Ст. 35 «Оценка эффективности мер по защите данных»* |
| Изменение приложений | » *Ст.15 «Право субъекта данных на доступ к данным*<br>» *Ст.16 «Право на исправление»*<br>» *Ст. 17 «Право на уничтожение» («право на забвение»)*<br>» *Ст. 18 «Право на ограничение обработки»*<br>» *Ст. 19 «Обязательное уведомление о внесении исправлений в персональные данные, уничтожении данных или ограничении обработки»*<br>» *Ст. 20 «Право на переносимость данных»* |
| Интеграция в архитектуру» | » *Ст. 32 «Безопасность обработки»*<br>» *Ст. 5 «Принципы обработки персональных данных»*<br>» *Ст. 24 «Ответственность контролера»*<br>» *Ст. 25 «Техническая и организационная защита данных»*<br>» *Ст. 28 «Обработчик данных»*<br>» *Ст. 34 «Оповещение субъекта об утечке персональных данных»* |

Создание и поддержание реестра данных является обязательным в соответствии со ст. 30 («Журнал обработки») GDPR и обычно становится отправной точкой любых действий, связанных со сбором и использованием персональных данных.

Снижение рисков является важной составляющей эффективной системы обеспечения ИТ-безопасности. Организации должны приложить усилия по предотвращению утечки персональных данных, для чего рекомендуется провести оценку безопасности и рисков. Чтобы узнать, как Oracle может помочь вам, свяжитесь с региональным представителем нашей компании.

В целях соблюдения определенных прав субъекта данных в соответствии со ст. 15–20 (например, «право на забвение») от вас может потребоваться внести ряд изменений в корпоративные процессы и приложения. Поскольку изменения вносятся в определенные приложения, позволяющие хранить данные субъекта, для реализации этой функции необходимо понимание конкретной модели данных и бизнес-логики.

Дополнительные меры могут быть приняты на уровне архитектуры, таком как шифрование сети или баз данных. Реализовать меры на уровне архитектуры обычно проще и дешевле, чем в приложении; также они, как правило, более эффективны, поскольку не ограничены моделью данных и бизнес-логикой. Этот подход к защите персональных данных может оказаться предпочтительным в крупных компаниях, где системы ИТ имеют сложную структуру, и сотрудники не всегда обладают необходимыми знаниями о приложениях.

## Решения Oracle для обеспечения безопасности и GDPR

Oracle предлагает широкий набор эффективных решений для обеспечения соответствия требованиям GDPR к реестру данных, информированности о рисках, изменению приложений и интеграции средств безопасности в архитектуру. На следующей диаграмме показана общая модель решений по информационной безопасности Oracle, которая включает в себя широкий набор продуктов и облачных сервисов.

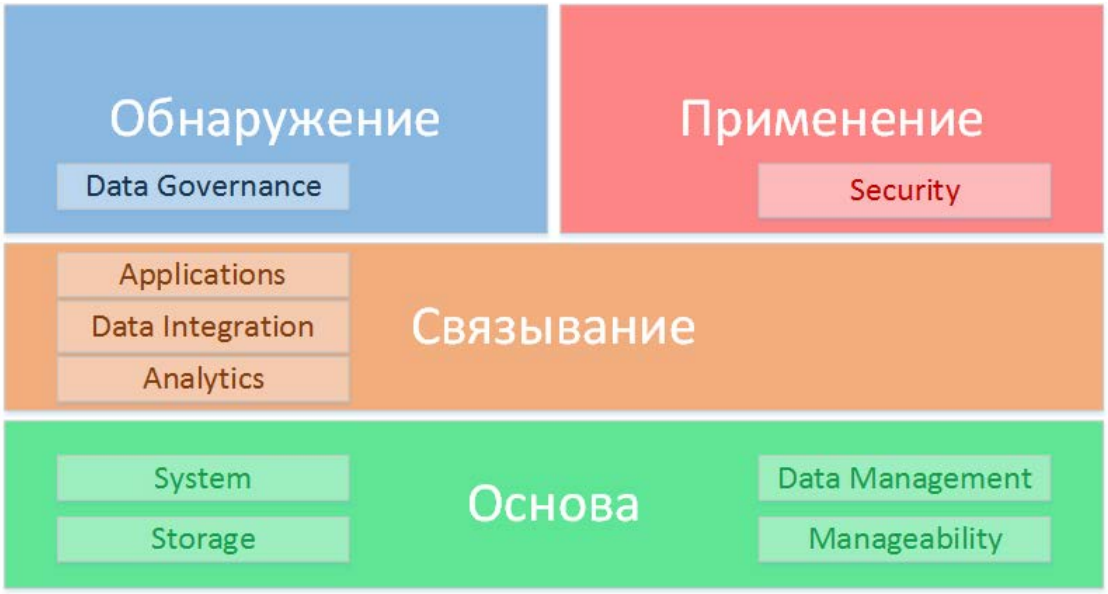


Рис. 1. Модель решений по информационной безопасности Oracle для GDPR.

**Обнаружение (Discovery)**. Локальные продукты и облачные сервисы для обнаружения персональной информации и составления схем потоков данных. Эта технология обеспечивает управление данными и включает в себя такие возможности, как отслеживание обработки данных, инвентаризация ресурсов и обнаружение данных.

**Связывание (Enrichment).** Связывание подразумевает внесение в приложения изменений, необходимых для обеспечения прав субъекта согласно ст. 15–20. Также может потребоваться консолидация данных клиента для обеспечения единого представления данных субъекта во всей организации.

**Основа (Foundation).** Комплексный набор надежных операционных технологий, которые являются неотъемлемой частью продуктов Oracle, эффективно обеспечивает безопасность ИТ без ущерба для доступности и производительности служб. Сюда относятся решения для гибридных облачных сред: от архитектуры максимальной доступности и инженерных систем до операционных систем и процессоров. Эти решения помогают обеспечить *«доступность и устойчивость обрабатывающих систем и служб, а также возможность своевременного восстановления доступности и предоставления доступа к данным в случае физического или технического инцидента»* (ст. 32).

**Применение (Enforcement).** Технологии Oracle для гибридного облака обеспечивают реализацию политик и мер безопасности для защиты пользователей, программного обеспечения и систем. Сюда относятся продукты и сервисы для прогнозирования, предотвращения, отслеживания и реагирования, обеспечивающие безопасность базы данных, управление идентификацией и доступом, а также средства мониторинга, управления и инструменты анализа поведения пользователей.

Следующий раздел документа содержит более подробную информацию об этих решениях. Дополнительные сведения о GDPR см. на веб-сайте: https://oracle.com/goto/gdpr.

## Решения для обеспечения безопасности (применение)

Согласно ст. 32 GDPR («Безопасность обработки») контролеры и обработчики данных должны принять меры по обеспечению уровня безопасности, соответствующего риску, который связан с обрабатываемыми данными.

В качестве примера таких мер защиты в статье упоминаются псевдонимизация и шифрование. **В соответствии с регламентом организация самостоятельно принимает решение о выборе мер для обеспечения конфиденциальности, целостности и доступности данных, отказоустойчивости их хранения и несет полную ответственность за внедрение системы безопасности.** Вопреки распространенному заблуждению, которым нередко пользуются поставщики решений безопасности, регламент не ограничивает средства защиты определенными технологиями. GDPR предусматривает ответственность для контролеров и обработчиков и требует от них оценить риски, связанные с использованием данных, и внедрить соответствующие защитные меры для их смягчения. Нередко организации пренебрегают даже самыми базовыми средствами обеспечения безопасности, к которым в том числе относятся следующие.

» Шифрование конфиденциальных данных при хранении и передаче.

» Своевременная установка системных исправлений.

» Проверка системных журналов для выявления аномальной активности.

» Ограничение прав или разделение обязанностей для привилегированных пользователей.

» Контроль распространения учетных записей пользователей и доступа к ним.

» Маскировка реальных данных, копируемых в среду разработки.

Раздел «Применение» модели безопасности Oracle включает в себя четыре группы решений, которые обеспечивают базовые средства защиты, рекомендуемые для использования в организации.

**Защита данных.** Шифрование хранящихся и передающихся данных является простым, но эффективным способом защиты и поэтому обычно становится одной из первых мер по созданию системы безопасности. Шифрование нередко используется для предотвращения несанкционированного доступа, оно не влияет на работу приложений и пользователей, обеспечивает эффективную профилактику нарушений и практически не снижает производительность современных решений. Дополнительные технологии защиты данных включают в себя управление ключами шифрования, редактирование данных на уровне приложений и маскировку конфиденциальных рабочих данных в средах для тестирования и разработки.

**Управление доступом.** Без внедрения средств управления доступом, определяющих, кто имеет право взаимодействовать с данными, шифрование не имеет смысла. Поэтому необходимо внедрить технологии управления доступом и учетными записями как для пользователей приложений, так и для ИТ-персонала, включая системных администраторов.

**Мониторинг, блокировка и аудит.** Сегодня, когда угрозы становятся все изощреннее, крайне важно использовать интеллектуальные автоматические средства для мониторинга инцидентов производительности и безопасности. Программные компоненты и приложения создают записи в журнале аудита. Необходимо собирать и анализировать данные о внутренних и внешних угрозах из различных источников, чтобы определять и снижать риски, предотвращая утечки данных.

**Настройки безопасности**. Чтобы гарантировать необходимый уровень безопасности, требуется регулярно устанавливать обновления и исправления для программного обеспечения и делать необходимые настройки. Управление настройками безопасности становится неотъемлемой составляющей передовых практик, поскольку киберпреступники все чаще используют уязвимости программного обеспечения для кражи конфиденциальных данных.

Четыре требования к безопасности, перечисленные ниже, используются во многих глобальных стандартах и распространенных методологиях, в том числе в семействе стандартов ISO 27000, NIST 800-53, PCI-DSS 3.2, OWASP и принципах киберзащиты Центра интернет-безопасности. Рассмотрим

подробнее раздел «Внедрение», представленный на рис. 1 «Модель решений по информационной безопасности Oracle для GDPR».


Рис. 2. Подробное представление раздела «Внедрение» модели решений по информационной безопасности Oracle

## Продукты Oracle для обеспечения безопасности, которые помогают соблюсти требования GDPR

Oracle предлагает продукты для защиты данных, управления учетными записями, а также мониторинга и аудита ИТ-среды, необходимые для обеспечения безопасности в локальных и облачных системах гибридной инфраструктуры. В таблице ниже приведены краткие описания продуктов, классифицированных по типу мер обеспечения безопасности. Описание включает в себя неполный перечень функций продукта. За дополнительными сведениями обратитесь к своему торговому представителю Oracle.

РЕШЕНИЯ ORACLE ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, ПОМОГАЮЩИЕ СОБЛЮСТИ ТРЕБОВАНИЯ GDPR

| Продукт Oracle | Меры безопасности | Облачная служба | Краткое описание |
|---|---|---|---|
| Advanced Security | Защита данных | | Прозрачное шифрование баз данных Oracle и редактирование конфиденциальных данных в приложениях |
| Key Vault | Защита данных | | Безопасное управление жизненного цикла ключей шифрования, паролей, сертификатов и др. |
| Data Masking and Subsetting | Защита данных | | Анонимизация реальных данных для сред тестирования и разработки. |
| Database Vault | Управление доступом | | Контроль доступа привилегированных пользователей по принципу предоставления минимально необходимых прав и разделения обязанностей. |
| Identity Cloud Service | Управление доступом | X | Управление учетными записями из облака для предоставления доступа к гибридной среде, авторизации, аутентификации, выделения ресурсов и единого входа. |
| Identity Governance | Управление доступом | | Управление жизненным циклом учетной записи: администрирование пользователей, управление привилегированными учетными записями и связанная с ними аналитика. |
| Access Management | Управление доступом | | Защита ИТ-ресурсов и федеративная идентификация для различных сценариев. |

| | | | |
|---|---|---|---|
| Directory Services | Управление доступом | | Управление крупными каталогами пользователей с быстро выполняющимися операциями «чтение-запись» |
| Label Security | Управление доступом | | Возможность присвоения отдельным записям ярлыков-метаданных и предоставление доступа на их основе. |
| Audit Vault and Database Firewall | Мониторинг, блокировка и аудит | | Централизованное управление аудитом, мониторингом, отчетностью и уведомлениями для обнаружения аномальной активности в базах данных. |
| Security Monitoring and Analytics Cloud Service | Мониторинг, блокировка и аудит | X | Мониторинг инцидентов безопасности в гетерогенных и гибридных облачных средах. |
| CASB Cloud Service | Мониторинг, блокировка и аудит | X | Обнаружение несанкционированных облачных сервисов и последовательное внедрение политик безопасности в контролируемых средах SaaS, PaaS и IaaS. |
| Configuration and Compliance Cloud Service | Соблюдение нормативных требований к безопасности | X | Внедрение средств для настройки ИТ-ресурсов и ее адаптации в соответствии с нормативными требованиями. |
| Enterprise Manager: Configuration Mgmt | Соблюдение нормативных требований к безопасности | | Проверка качества и безопасности установки и настройки ИТ-ресурсов. |

В качестве первоначальной меры Oracle рекомендует установить Oracle Advanced Security с функцией прозрачного шифрования в соответствии с передовыми рекомендациями и для защиты важных сведений, которые часто содержатся в базах данных.

## “Data Protection by Design”

Одной из важнейших концепций GDPR является «техническая и организационная защита данных» в соответствии со ст. 25, которая гласит, что *«необходимо применять соответствующие технические и организационные меры — как при определении средств обработки, так и во время самой обработки»*. Концепция технической защиты данных перекликается с концепцией «безопасности по умолчанию» Oracle, которая подразумевает перенос политик и средств управления ближе к данным.

Внедрение решений Oracle (см. таблицу 1) в рамках интеграции архитектуры имеет следующие преимущества.

» Упрощенные средства обеспечения безопасности в рамках проверенных технологий Oracle.

» Установка обновлений и исправления для программного обеспечения.

» Устранение потребности в разработке, часто сопряженной с возникновением системных и программных ошибок, которые могут стать причиной утечки данных.

## Пример использования

Следующий пример иллюстрирует применение решений Oracle для повышения безопасности ИТ-систем и обеспечения соответствия требованиям GDPR по защите данных ЕС.

### Сфера применения – здравоохранение

Рассмотрим в качестве примера вымышленную организацию, представляющую собой крупную частную клинику. Рынок частных медицинских услуг консолидируется, и наша организация недавно присоединила к себе другую компанию, оказывающую услуги диагностики и краткосрочной

госпитализации в ряде городов. Приобретенная компания также росла за счет слияний, но в более скромных масштабах.

По результатам слияния был начат проект со следующими бизнес-целями.

» Объединение баз клиентов для проведения общих и специализированных маркетинговых мероприятий по продвижению услуг профилактической диагностики.

» Повышение качества обслуживания при записи на прием (через Интернет или мобильные устройства) и получения медзаключений.

» Соблюдение национальных и региональных законов, в том числе GDPR.

» Создание репутации современной компании, заботящейся о безопасности и защите конфиденциальности данных пациентов.

Также были поставлены следующие цели в сфере ИТ:

» Модернизация разрозненных ИТ-систем (последствие нескольких слияний) с сохранением целостности бизнеса.

» Добавление средств управления учетными записями сотрудников (врачи, медсестры, администраторы и т. д.) и возможностей единого входа с целью сократить риск мошенничества и административную нагрузку.

По техническим причинам организация не желает проводить одновременную замену систем: некоторые из них будут модернизированы позднее, другие будут обновляться постепенно. В организации используются пакетные приложения от независимых поставщиков. Компания-разработчик одного из этих приложений обанкротилась и не может предоставлять услуги по обслуживанию и обновлению программного кода. Кроме того, организация использует услуги сторонней компании в локальных центрах обработки данных, которые включают в себя обслуживание оборудования, сети, операционных систем и СУБД Oracle, и продолжит использовать их на протяжении как минимум ближайших двух лет.

**Разработка плана**

Изначально руководство организации считало, что введение GDPR препятствует достижению их бизнес-целей, однако генеральный директор обнаружил, что они согласуются с требованиями эффективности и безопасности ИТ-систем. Выполнив необходимый анализ, организация приступила к внедрению средств безопасности на уровне архитектуры и постепенно смогла реализовать поставленные цели для бизнеса и ИТ.

**Используемые технологии**

Прежде всего требовалось определить место хранения конфиденциальных персональных данных. Для баз данных Oracle интеграция выполнялась с помощью модуля Application Data Model (ADM). ADM хранит список приложений, таблиц и связей между столбцами таблиц, которые заявлены в словаре данных, импортируются из метаданных приложения или указываются пользователем.

Затем необходимо было оценить состояние безопасности в организации. Прибегнув к услугам Oracle Consulting для оценки безопасности баз данных Oracle, организация провела опрос сотрудников и подрядчиков ИТ и применила средства оценки (такие как Database Security Assessment Tool и бета-версия сервиса Configuration and Compliance Cloud Service). По результатам оценки был составлен отчет, ставший основой для плана внедрения корректирующих мер и необходимых технологий. На выполнение всех этих действий потребовалось меньше недели. Отчет по результатам оценки был сохранен как ключевой компонент проекта по выполнению организацией требований GDPR (в

соответствии со ст. 24) и представлен совету директоров специалистом по безопасности данных.

В отчете были выделены следующие важные корректирующие меры.

» **Отказ от использования неподдерживаемых версий Oracle Database 10 и 9 и переход на Oracle Database 12c.** Организация обратилась к поставщикам приложений для сертификации новой версии, но в случае с обанкротившимся поставщиком это было невозможно. Перенос базы данных не был производен, однако в качестве компенсации был внедрен брандмауэр Oracle для баз данных, входящий в состав решения Oracle Audit Vault and Database Firewall.

» **Внедрение средств шифрования и управления доступом.** Организация приняла решение о шифровании данных в базе с помощью Oracle Advanced Security (в соответствии со ст. 32). С помощью решения Oracle Database Vault был выполнен анализ привилегий учетных записей и были созданы персональные учетные записи с ограниченным доступом по принципу минимально необходимой осведомленности. В ходе проверки было обнаружено, что пароли системных администраторов не менялись в течение нескольких лет.

» **Централизация учетных записей пользователей БД.** Организация внесла все учетные записи пользователей базы данных в единый каталог с помощью функции Enterprise User Security и существующего экземпляра каталога Oracle.

» **Маскировка данных в нерабочих средах.** Организация решила запретить копирование реальных рабочих данных в среду для разработки и тестирования. В связи с этим были приняты следующие меры: разработчикам были предоставлены системы, не содержащие данных, и в организации была внедрена технология маскирования Oracle Data Masking and Subsetting.

» **Возврат к использованию механизмов протоколирования, не применявшихся в течение нескольких лет.** Ведение журналов и анализ событий являются основой стратегии безопасности. Организация использовала Oracle Audit Vault для ведения журналов баз данных и Oracle Log Analytics Cloud Service — для журналов системных событий. Затем был использован Oracle Storage Cloud Service для уменьшения нагрузки Audit Vault на локальные системы и в качестве хранилища для журналов приложений. Некоторые приложения были изменены, чтобы обеспечить передачу пользовательских данных в базу и улучшить предоставление отчетности и анализ журналов.

Параллельно организация интегрировала использующийся портал с Oracle Identity Cloud Service (IDCS), чтобы улучшить качество обслуживания клиентов и повысить уровень безопасности с помощью функций единого входа, надежной аутентификации и адаптивного доступа. Та же технология использовалась для предоставления функций аутентификации и единого входа внутренних пользователей. Учетные записи были синхронизированы с локальной службой Active Directory. На завершающем этапе организация приступила к сокращению числа учетных записей в локальных системах и централизации.

Организация начала использовать облачный сервис Oracle CASB (Cloud Access Security Broker) для мониторинга несанкционированного использования облачных служб в корпоративной сети. Это позволило предотвратить кражу персональных данных из облака и осуществлять мониторинг почтовых служб Microsoft. Развертывание сервисов и внедрение их в рабочую среду заняло одну неделю. Организация решила использовать технологию Oracle Identity SOC, объединяющую в себе сервисы Oracle Identity, CASB, Security Monitoring and Analytics и Configuration and Compliance Cloud Services, и отказаться от услуг стороннего поставщика, за исключением сетевого операционного центра. Эксперты Oracle предложили организации в дальнейшем прибегнуть к услугам той же компании для выполнения анализа, предварительно внедрив Identity SOC в качестве более современного и функционального решения, позволяющего в том числе управлять отзывом ролей и полномочий.

## Заключение

Несоблюдение требований GDPR может вести к крупным штрафам и наложению взысканий. Что еще более важно, значительные нарушения могут нанести ущерб бренду, стоимости и репутации компании. Организация, занимающаяся сбором персональных данных, всегда должна быть в состоянии убедительно продемонстрировать соответствие требованиям регламента и принципам безопасности.

Приведение деятельности организации в соответствие GDPR включает в себя создание координированной стратегии, затрагивающей юридический, кадровый, маркетинговый отделы, службы ИТ и безопасности и др. Организации должны разработать четкую стратегию и план действий и обеспечить соответствие требованиям GDPR не позднее 25 мая 2018 г.

Мы предлагаем нашим клиентам воспользоваться многолетним опытом и технологическими возможностями Oracle, чтобы упростить этот процесс. Чтобы узнать, как Oracle может помочь вам, свяжитесь с региональным представителем нашей компании или посетите веб-сайт https://oracle.com/goto/gdpr.

ORACLE

**Корпорация Oracle, головной офис**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Для международных запросов**
Тел.: +1.650.506.7000
Факс: +1-650-506-7200

СЛЕДИТЕ ЗА НАШИМИ НОВОСТЯМИ

blogs.oracle.com/oraclesecurity
facebook.com/oraclesecurity
twitter.com/oraclesecurity
oracle.com/security

Integrated Cloud Applications & Platform Services



Использование решений Oracle для обеспечения безопасности в соответствии с Общим регламентом по защите данных (GDPR)
Июль 2017
Автор: Alessandro Vallega, Troy Kitch
Соавторы: Angelo Bosis