

Оценка соответствия нормам GDPR

Регламент General Data Protection Regulation (GDPR) должны соблюдать все организации, обрабатывающие персональные данные субъектов, **находящихся** на территории ЕС, в т.ч. граждан РФ.

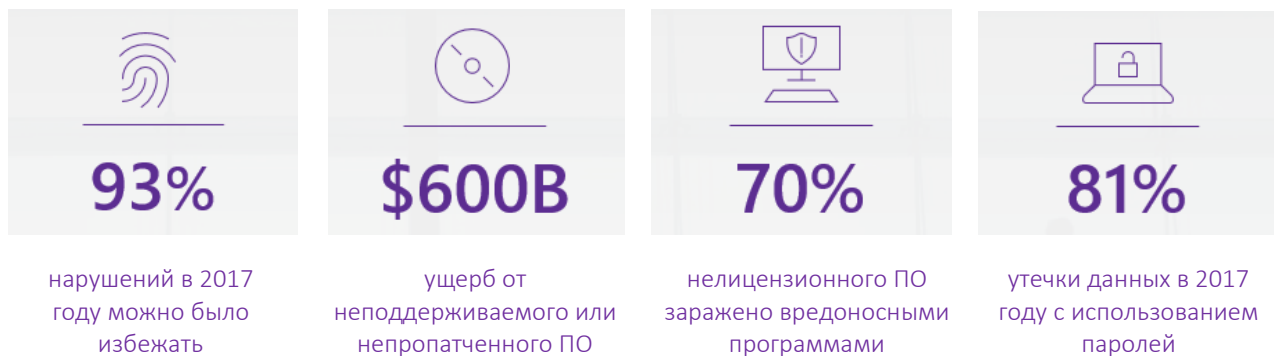
Под требования GDPR попадают:

- Дочерние общества крупных российских холдингов – торговые предприятия компаний-экспортеров, находящиеся на территории ЕС.
- Компании банковского и телекоммуникационного сектора.
- Компании, предоставляющие услуги потребителям из ЕС: интернет-магазины, гостиницы, авиакомпании-перевозчики, компании по предоставлению логистических услуг.

Возможный ущерб:

- штраф до **€20,000,000** или
- **4%** от годовой прибыли компании
- а также запрет на обработку ПД, закрытие компании, запрет директору занимать руководящие должности в течение 3 и более лет

Управление активами - основа для соответствия GDPR и обеспечения кибербезопасности



Продолжительность проекта: 1-3 месяца

Этапы:



Проект GDPR предоставляет комплексный анализ инфраструктуры, обеспечивает обнаружение неуправляемых и уязвимых устройств в ИТ-инфраструктуре и дает рекомендации для повышения кибербезопасности и сохранности персональных данных.

Обеспечьте соответствие нормам GDPR и кибербезопасность:

Определите способы доступа и использования персональных данных	Примите меры безопасности для предотвращения и обнаружения утечки данных
Защитите критически важные сегменты инфраструктуры	Обеспечьте целостность, доступность и конфиденциальность данных
Проведите оценку рисков систем и ПО на предмет потенциальных угроз для конфиденциальности данных субъектов	Реагируйте на уязвимости. Определите области риска и обеспечьте соответствие требованиям и безопасность

Конфиденциальность и безопасность объединены и требуют организационных изменений. В ходе проекта оцениваются организационный и технический уровни:

Традиционная среда	Среда с обеспечением конфиденциальности
Бизнес / Коммерческая стратегия	Стратегия конфиденциальности
Общее понимание безопасности	Общеорганизационная культура безопасности и конфиденциальности
Узкоспециализированные отношения с бизнес-партнерами/поставщиками	Предварительно подготовленные (обрабатываемые) соглашения
Фокус на бизнес-приложениях как активах	Фокус на данных как активе компании
Индивидуально определенный доступ на основе групп безопасности	Обоснованные доказательства доступа на основе бизнес-ролей с проверками / аудитами
Практика обеспечения безопасности для защиты ИТ-активов	Защита данных для обеспечения конфиденциальности данных

Результаты:

1. Комплексная оценка и рекомендации по процессам управления критическими данными, с учетом внедренных практик на организационном и техническом уровнях
2. Оценка и рекомендации для повышения кибербезопасности по критическим направлениям на основе международного свода рекомендаций CIS Controls
3. План ближайших шагов по устранению наиболее критичных уязвимостей
4. Дорожная карта по внедрению передовых решений для построения гибкой ИТ инфраструктуры, быстро реагирующей на возникающие угрозы
5. Построение модели зрелости, соотносящейся со статьями регламента GDPR – оценка обеспечения конфиденциальности, безопасности и минимизации риска раскрытия ПД
6. Рекомендации для улучшения управления и защиты ПД и соответствия требованиям GDPR

Преимущества работы с нами:

- Реализуем комплексные проекты оптимизации ИТ-инфраструктуры: от аудита и постановки задачи до внедрения и обучения пользователей
- Имеем собственную методологию проектов оптимизации инвестиций в ПО
- Разработчики ГОСТ Р ИСО/МЭК 19770-1-2014 (ISO/IEC 19770-1).
- Финалист международного конкурса Microsoft Partner of the Year 2018, 2016
- Победитель российского конкурса партнерских ИТ-решений Microsoft в номинации SAM 2016

Свяжитесь с нами:

Наталья Галкина
 Ведущий консультант
galkina@iterbi.ru