КАК НЕ ДОПУСТИТЬ ОБОРОТНЫХ ШТРАФОВ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Денис СУХОВЕЙ
директор продуктового направления защиты данных компании «Аладдин Р.Д.»

Анна ГОРШКОВА
product marketing manager компании «Аладдин Р.Д.»

30 ноября 2024 г. Президент Российской Федерации подписал Федеральный закон № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», который вступит в силу 30 мая 2025 г.

Какие меры предусмотрены для компаний за утечку персональных данных?

С момента вступления в силу изменений компаниям-операторам персональных данных могут быть предъявлены следующие штрафы:

- **до 300 тыс ₽** за несвоевременное уведомление Роскомнадзора о намерении начать обработку персональных данных (далее ПДн);
- **до 3 млн ₽** за каждую просрочку уведомления об утечке и промедление уведомления о результатах внутреннего расследования утечки;
- **до 500 млн ₽** за утечку ПДн;
- **до 10 лет лишения свободы** за незаконное использование ПДн.

Новые меры за нарушение работы с ПДн очень строгие, срок до вступления изменений в силу короткий. При оценке инцидента и вынесении наказания за утечку законодательство предусматривает смягчающие меры. Но их наличие не освобождает компанию от ответственности. Из всего многообразия ИБ-инструментов сейчас организациям необходимо выбирать защиту непосредственно самих данных.

В чём причины ужесточения наказания за утечку данных?

При общем росте уровня информационной безопасности в крупных российских организациях вопросу непосредственно защиты данных уделяется мало внимания. Все силы сосредоточены на защите инфраструктуры и управлении ИБ-инцидентами — защита периметра, мониторинг событий, управление контролем доступа. Эти меры важны для снижения уровня угроз, но сами данные не защищают. Персональные данные стали современной валютой, при организации целевых атак именно они являются мишенью для злоумышленников. По разным оценкам вероятность успеха атак, целью которых является похищение данных достигает 90 %. Когда злоумышленники доберутся до желаемой цели — лишь вопрос времени. Такой масштаб проблемы побудил государство ужесточить регулирование, давая участникам рынка прямой сигнал — **утечки персональных данных должны прекратиться**. На языке информационной безопасности это означает, что обеспечение конфиденциальности персональных данных является приоритетной задачей защиты информации для любой организации.

Как предотвратить угрозы утечек и обеспечить конфиденциальность персональных данных?

Организации-оператору ПДн необходимо выделить информационные системы, обрабатывающие наибольшие объёмы персональных данных. Обычно это одна-две системы, данные которых коммерчески привлекательны для злоумышленников. Затем необходимо определиться с мерами защиты конфиденциальности этих систем. Наиболее эффективным методом защиты персональных данных является их обезличивание. Обезличивание позволяет организации использовать важную информацию в своих рабочих процессах, но при этом делает её абсолютно бесполезной для злоумышленников. Инструментом такой защиты является российский программный продукт Крипто БД, механизмы которого основаны на отечественных криптоалгоритмах, соответствующих требованиям ФСБ России к СКЗИ. Селективное прозрачное шифрование является эффективным и, пожалуй, единственно действенным методом предотвращения масштабных утечек данных. Система Крипто БД представляет собой набор важнейших возможностей для ИБ-специалиста:

- **обезличивание данных выборочным шифрованием таблиц/столбцов базы данных;**
- **«прозрачность» для пользователей и приложений;**
- **двухфакторная аутентификация и контроль доступа;**
- **централизованное управление;**
- **мониторинг и аудит.**

Введение оборотных штрафов за масштабные утечки персональных данных безусловно изменит приоритеты большинства компаний. Широкое применение продукта Крипто БД показывает, что такой подход к защите информации в СУБД обходится организации существенно дешевле (время, деньги, трудозатраты), чем организация внушительного состава комплексных мероприятий, дающих лишь робкую надежду, что злоумышленник не проберётся через несколько эшелонов периметровой безопасности, до хранилища незащищённых данных.