КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург, ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

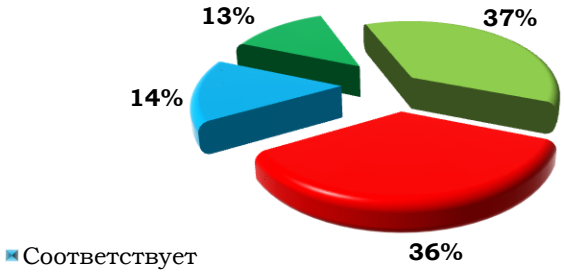
Персональные данные. Новые требования и практические рекомендации

Практика последних лет показывает, что вопреки мнению скептиков, вопросы защиты персональных данных не теряют своей актуальности. Инциденты, связанные с раскрытием персональных данных и сведений о личной жизни граждан, незаконным использованием таких сведений третьими лицами, наносящим ущерб гражданам, продолжают находить свое отражение в СМИ.

Рост осведомленности и юридической грамотности граждан в вопросах соблюдения их прав заставляет многих руководителей принимать решение о реализации необходимого комплекса мер по организации обработки персональных данных в соответствии с законодательными требованиями. Защита персональных данных сотрудников и клиентов становится элементом корпоративной культуры повсеместно.

Вступление в силу Постановления Правительства РФ от 01.11.2012 г. №1119 и детализирующего его положения Приказа ФСТЭК от 18.02.2013 г. №21 требует от Операторов персональных данных пересмотра реализованного у них комплекса мер по организации обработки и защиты персональных данных.

Новые требования к защите персональных данных в информационных системах персональных данных



Из 109 мер, предусмотренных Приказом ФСТЭК №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»:

- ✓ 40 являются рекомендуемыми (компенсирующими, дополнительными);
- ✓ 30 полностью или частично соответствуют ранее существовавшим требованиям;
- ✓ **39 являются абсолютно новыми.**

В условиях действия новых требований к защите персональных данных в ИСПДн КонсалтИнфоМенеджмент рекомендует:

1. Пересмотреть модель угроз информационной безопасности ИСПДн в части, касающейся актуальности угроз недекларированных возможностей в прикладном и системном программном обеспечении ИСПДн.
2. Определить необходимый уровень защищенности ПДн при из обработке в ИСДПн с документальным оформлением соответствующего акта.
3. Провести анализ действующей в компании системы защиты персональных данных на предмет ее соответствия новым требованиям с оформлением соответствующего заключения.
4. Разработать и реализовать план приведения системы защиты персональных данных в соответствие требованиям приказа ФСТЭК от 18.02.2013 г. №21.

Статистика

С момента вступления в силу Федерального закона №152-ФЗ регуляторами было проведено несколько тысяч проверок соответствия процессов обработки и защиты ПДн. **Свыше 90%** всех проверок были осуществлены Роскомнадзором

Ввиду особенностей сферы ответственности Роскомнадзора, подавляющее большинство выявленных нарушений приходится не на техническую защиту персональных данных, а на организацию порядка обработки персональных данных — определение необходимости взятия согласия с субъекта, порядка допуска и ознакомления сотрудников, ознакомление клиентов с их правами, организация передачи персональных данных третьим лицам, наличие порядка реагирования на запросы различных категорий субъектов ПДн.

Вопрос - Ответ

В: ***В нашей компании уже была проведена классификация ИСПДн по Приказу №55/86/20. Зачем нам нужно проводить классификацию еще раз?***

О: «Приказ трех» №55/86/20 и Приказ ФСТЭК №58 утратили силу. Классификация действующих ИСПДн и определение требований к их защите должны осуществляться на основании новых нормативных методических документов. Практика показывает, что некоторые территориальные подразделения Роскомнадзора уже требуют при проверках акты определения уровней защищенности, несмотря на наличие актов классификации в соответствии с «приказом трех».

Сведения для Операторов ПДн, реализовавших меры по организации обработки и защиты ПДн до 25.07.2011 г.

Федеральный закон №ФЗ-261 от 25.07.2011 г. внес существенные изменения в №152-ФЗ «О персональных данных». В частности, теперь Операторы ПДн должны:

1. назначить Ответственного за организацию обработки ПДн (ст.18, п.1);
2. разработать и опубликовать документ, определяющий политику обработки ПДн (ст. 18, п.2 ФЗ-152 в ред. 25.07.2011г.);
3. реализовать организационные и технические меры по обеспечению безопасности ПДн в соответствии со статьей 19 ФЗ-152;
4. осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям законодательства (ст.18, п.4 в ред. 25.07.2011г);
5. оценить возможный вред субъекту ПДн (ст. 18, п.5 в ред. 25.07.2011г);
6. разработать нормативные документы, регламентирующие процедуры обработки и защиты ПДн и ознакомить с ними работников (ст.18, п.2 и п.6);
7. принять меры по удалению или уточнению неполных или неточных ПДн (ст. 5, ч.6 в ред. 25.07.2011г).

Что может предложить КонсалтИнфоМенеджмент?

1. Проведение оценки соответствия процессов обработки и защиты ПДн требованиям законодательства.

Позволяет Оператору получить необходимое представление о текущем и необходимом уровне соответствия требованиям законодательства в сфере защиты ПДн и рекомендации по приведению этих процессов в соответствие.

2. Разработка пакета нормативной и организационно-распорядительной документации, регламентирующей порядок обработки персональных данных.

Позволяет регламентировать порядок обработки ПДн в компании и внедрить процедуры взаимодействия с субъектами ПДн (сбор, хранение, передача третьим лицам, реагирование на запросы).

3. Осуществление полного комплекса работ по приведению в соответствие Федеральному закону №152-ФЗ «О персональных данных» (организационные и технические мероприятия).

Позволяет снизить риски информационной безопасности, в том числе минимизировать возможность нарушения прав субъектов ПДн и возникновения замечаний со стороны регуляторов.

Наш опыт

За период с 2009 года по настоящий момент командой успешно реализовано более 40 проектов в сфере организации обработки и защиты персональных данных. На объектах наших клиентов Регуляторами было проведено 8 проверок (6-Роскомнадзор, 2 - ФСТЭК). Проверки пройдены успешно. Серьезных замечаний получено не было.

О компании

КонсалтИнфоМенеджмент - оператор услуг системной интеграции и консалтинга в области информационной безопасности. Деятельность компании охватывает широкий спектр услуг, связанных с автоматизацией бизнес-процессов, защитой информации и обеспечением выполнения требований законодательства РФ и международных стандартов по защите информации.

Полное описание наших услуг, перечень лицензий Вы можете найти на сайте КонсалтИнфоМенеджмент http://www.km-ltd.ru/

Вопрос - Ответ

В: ***Нашей организации нет в реестре плановых проверок, внеплановые тоже пока не предвидятся. Зачем нам организовывать работы по защите ПДн до проверки?***

О: Для качественного выполнения работ по защите персональных данных требуется провести обширный комплекс мероприятий, включающий выявление бизнес-процессов Оператора, затрагивающих обработку ПДн, разработку моделей угроз и нарушителя, определение уровней защищенности ИСПДн, разработку и внедрение организационно-распорядительных документов, разработку системы защиты ПДн, реализацию технических и организационных мероприятий, разрешительной системы доступа, приобретение, пуско-наладку и специальную настройку средств защиты информации и т. д. Реализация всех этих мероприятий требует времени, поэтому к вопросу организации обработки и защиты ПДн стоит подойти заранее.

Проведение внеплановой проверки (в соответствии с административным регламентом проведения проверок Роскомнадзора, приказ от 1.12.2009 г., №630) соответствия обработки персональных данных требованиям законодательства РФ в области персональных данных может быть инициировано по обращениям субъектов персональных данных (клиентов, работников), в случае нарушения их прав и законных интересов действиями (бездействием) Операторов при обработке их персональных данных.

Вопрос - Ответ

В: ***В нашей компании обрабатываются исключительно персональные данные работников, мы не являемся оператором персональных данных - государственные регуляторы не имеют права проверять нас!***

О: В случае обращения гражданина о нарушении его прав и законных интересов при обработке персональных данных, может быть инициирована внеплановая проверка любого лица, допустившего такое нарушение. Так, согласно отчету о деятельности Роскомнадзора за 2012 год, в адрес органов прокуратуры по результатам рассмотрения обращений граждан направлен 751 материал для решения вопроса о возбуждении дел об административных правонарушениях, предусмотренных ст. 13.11 КоАП РФ.

КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург, ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64