

Обеспечение безопасности персональных данных

Компания Открытые Технологии предлагает своим клиентам пакет услуг по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах (ИС).

ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

Декларация неприкосновенности частной жизни, личной и семейной тайны граждан РФ приводится в Конституции Российской Федерации.

ФЗ № 152-ФЗ «О персональных данных», принятый в июле 2006 г., обязывает операторов персональных данных «принять необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

Под действие этого закона попадают все операторы персональных данных, как государственные учреждения, так и коммерческие предприятия и организации, в ИС которых осуществляется автоматизированная обработка персональных данных.

Детальные требования по защите персональных данных (ПДн), обязательные для выполнения, приводятся в подзаконных нормативно-правовых и нормативно-методических документах, разрабатываемых Правительством РФ, ФСТЭК и ФСБ России.

Перечень защитных мер дифференцирован и зависит от установленного класса информационной системы, в которой обрабатываются персональные данные, а также актуальных угроз, направленных на нарушение защищаемых свойств ПДн. Класс информационной системы выбирается в соответствии с Таблицей 1.

Категория ПДн, обрабатываемых в ИС	Объем ПДн, обрабатываемых в ИС		
	В ИС одновременно обрабатываются ПДн менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации	В ИС одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе госвласти, проживающих в пределах муниципального образования	В ИС одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом
Обезличенные и (или) общедоступные ПДн	K4	K4	K4
ПДн, позволяющие идентифицировать субъекта ПДн	K3	K3	K2
ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию	K3	K2	K1
ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	K1	K1	K1

Таблица 1.

В общем случае компании, ИС которых отнесены к классам К1, К2, К3, должны:

- создать систему защиты ИС, в которой осуществляется обработка персональных данных, и провести оценку ее соответствия установленным требованиям;
- получить лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации;
- осуществить работы по защите речевой конфиденциальной информации (в случае воспроизведения персональных данных по акустическому каналу).

Ответственность за нарушение требований в области защиты персональных данных установлена в Кодексе РФ об административных правонарушениях (КоАП ст. 13.12, 13.13, 19.5) - наложение штрафа на должностное лицо или компанию до 500 000 рублей с возможной конфискацией средств защиты информации и приостановлением деятельности компании на срок до 90 суток. Наказание также предусматривает и Уголовный кодекс РФ (УК ст.137, 171) - штраф 300 000 рублей, арест до 6 месяцев и лишение права занимать должность на срок до 5-ти лет.

РЕШЕНИЕ КОМПАНИИ ОТКРЫТЫЕ ТЕХНОЛОГИИ

В рамках предлагаемого пакета услуг компания Открытые Технологии проводит работы по созданию системы защиты ИС, в которой осуществляется обработка персональных данных.

Создаваемая система защиты представляет собой совокупность организационных мер (процессов информационной безопасности (ИБ)), а также технических и программных средств защиты информации.



Создание систем защиты ИС, обрабатывающих персональные данные, осуществляется в несколько этапов.

На первом этапе проводится обследование информационной системы, ее классификация и задание конкретных требований по обеспечению безопасности ПДн.

На втором этапе проектируется система защиты ИС – разрабатываются необходимые проектные, эксплуатационные и организационно-распорядительные документы по обеспечению информационной безопасности.

На третьем этапе осуществляется внедрение системы защиты ИС. Проводится поставка необходимых средств обеспечения ИБ и их пуско-наладка, обучение персонала компании по вопросам защиты информации, внедрение разработанных процессов ИБ (организационных мер). При создании систем защиты информационных систем, содержащих персональные данные, используются средства ИБ как российских так и зарубежных производителей, в том числе, в требуемых законодательством случаях, имеющие необходимые сертификаты регуляторов в области ИБ (ФСБ, ФСТЭК России и др.).

На последнем этапе создания системы защиты ИС, в которой обрабатываются персональные данные, оценивается ее соответствие установленным требованиям по ИБ путем проведения внешнего аудита (аттестации) и оказывается содействие в получении документов, разрешающих осуществлять обработку персональных данных. Кроме того, в зависимости от установленного класса ИС, в рамках данного пакета услуг компания Открытые Технологии может провести:

- работы по оказанию методической помощи в получении лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации;
- работы по защите речевой конфиденциальной информации – создание в компании защищаемых помещений, предназначенных для ведения конфиденциальных переговоров.

Системный интегратор имеет все необходимые лицензии для осуществления данного вида деятельности, а также штат высококвалифицированных специалистов и большой практический опыт реализации проектов в области обеспечения безопасности персональных данных.

РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Компания Открытые Технологии ведет проекты по обеспечению безопасности персональных данных в соответствии с требованиями следующих основных документов:

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Указа Президента Российской Федерации от 17.03.08 г. №351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановления Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.08 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- Нормативно-методических документов ФСТЭК России от 15 февраля 2008 г. «Основные мероприятия по организации...», «Рекомендации по обеспечению безопасности...», «Базовая модель угроз безопасности...», «Методика определения актуальных угроз безопасности...»;
- Нормативно-методических документов ФСБ России от 21 февраля 2008 года «Методические рекомендации...», «Типовые требования...».

ВЫГОДЫ ДЛЯ БИЗНЕСА

В результате реализации проекта в области защиты персональных данных наши клиенты получают следующие преимущества:

Снижение рисков, связанных с регуляторами

Объективное повышение уровня ИБ информационной системы

Получение дополнительного конкурентного преимущества на рынке

Повышение доверия к компании со стороны клиентов и партнеров

Компания Открытые Технологии имеет богатый опыт успешно реализованных проектов области информационной безопасности, включающих в себя полный цикл работ – от предпроектного обследования до оказания технической поддержки. Компетенции специалистов компании подтверждены ведущими мировыми производителями программного и аппаратного обеспечения. Накопленный опыт, наличие квалифицированного персонала, тесное взаимодействие всех отделов позволяют компании уверенно браться за решение новых задач любой сложности.

Более подробную информацию можно получить по телефону: +7 (495) 787-08-88, или отправив запрос по адресу security-info@ot.ru.

www.ot.ru