АНТИВИРУСНЫЙ ЦЕНТР®

АНТИВИРУСНЫЙ ЦЕНТР

ДИСТРИБУЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И IT-УСЛУГ

+7 (495) 921-4008 www.AntiVirusPro.com uslugi_d@antiviruspro.com

АНТИВИРУСНЫЙ ЦЕНТР

Обеспечение соответствия требованиям к защищенности персональных данных

Практические пути достижения соответствия

Сергей Золотухин
Руководитель направления
Дистрибуции услуг
ООО «Антивирусный Центр»

Обеспечение безопасности ПДн

Оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

АНТИВИРУСНЫЙ ЦЕНТР

Организационные и технические мероприятия

Уведомление (ст.22 ФЗ-152)

1. Подача уведомления об обработке персональных данных (ст.22 ФЗ-152)

Уведомление должно содержать следующие сведения:

- наименование и реквизиты оператора
- цель обработки ПДн
- категории ПДн
- категории субъектов, ПДн которых обрабатываются
- правовое основание обработки ПДн
- перечень действий с ПДн, общее описание используемых оператором способов обработки ПДн
- описание мер, которые оператор обязуется осуществлять при обработке ПДн, по обеспечению безопасности ПДн при их обработке
- перечень средств обеспечения безопасности
- дата начала обработки ПДн
- срок и условие прекращения обработки ПДн

Пример. Уведомление не предоставлено

27.12.2010

Управление Роскомнадзора по Республике Коми провело внеплановые контрольно-надзорные мероприятия в отношении Обществ с ограниченной ответственностью Управляющая компания «ЖилВест» и «Жилищная Управляющая Компания» (г. Сыктывкар).

В ходе проверок выявлены нарушения обязательных требований…, а именно непредставление в Управление Роскомнадзора по Республике Коми уведомления об обработке персональных данных.

Пример. Уведомление не полное.

1 марта 2011 года

Управление Роскомнадзора по Костромской области в ходе плановой проверки Департамента ЖКХ Костромской области выявило нарушения законодательства в сфере персональных данных.

Департаментом представлены неполные сведения в уведомлении об обработке персональных данных …

Материалы направлены в Прокуратуру Костромской области для принятия решения о возбуждении дела об административном правонарушении

Основные организационно-технические мероприятия

2. Получение оператором согласия субъекта ПДн на обработку, за исключением случаев, предусмотренных частью 2 ст. 6 ФЗ-152
3. Уведомление субъекта ПДн о прекращении обработки его ПДн в случае достижения цели обработки его ПДн, а также в случае устранения допущенных нарушений или об уничтожении ПДн (ст. 21 ФЗ-152)
4. Разработка Положения (Регламента) правил обработки ПДн, осуществляемых без использования средств автоматизации с указанием различных форм и журналов, в которых предполагается или допускается включение ПДн (постановление Правительства РФ от 15.09.2008 № 687)
5. Получение письменного согласия работника на получение и обрабатывание его ПДн (п.3 ст. 86 ТК РФ)
6. Приказ о назначении сотрудников ответственных за обработку ПДн (постановление Правительства РФ от 17.11.2007 № 781)
7. Утвержденный список лиц, допущенных к ПДн для выполнения служебных (трудовых) обязанностей (постановление Правительства РФ от 17.11.2007 № 781)

Основные организационно-технические мероприятия

8. Приказ о составе комиссии по классификации и классификация информационных систем ПДн (приказ ФСТЭК/ФСБ/Мининформсвязи России от 13.02.2008 № 55/86/20)

Класс типовой информационной системы	< 1000 или в пределах одной организации	> 1000 или обрабатывает отрасль, орган гос.власти или муниципальный район	> 100000 или охватывает субъект РФ и более
категория 4 - обезличенные и (или) общедоступные персональные данные	К4	К4	К4
категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных	К3	К3	К2
категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1	К3	К2	К1
категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни	К1	К1	К1

Основные организационно-технические мероприятия

9. Составить перечень технических средств, участвующих в обработке ПДн (п.12 постановления Правительства РФ от 17.11.2007 № 781)
10. Создать электронный журнал обращений на получение ПДн (п.15 постановления Правительства РФ от 17.11.2007 № 781)
11. Разработать частную модель угроз безопасности ПДн, а также модель нарушителя в случае использования криптографических средств (п.12 постановления Правительства РФ от 17.11.2007 № 781)
12. Разработать должностные инструкции в части обеспечения безопасности ПДн при их обработке (п.12 постановления Правительства РФ от 17.11.2007 № 781)
13. Организация порядка резервного копирования ПДн на внешние носители (п.11 постановления Правительства РФ от 17.11.2007 № 781)
14. Проведение контрольных мероприятий, направленных на обеспечение уровня защищенности ПДн (п.11 постановления Правительства РФ от 17.11.2007 № 781)
15. Разработка частного технического задания и технического проекта на создание системы защиты (п.12 постановления Правительства РФ от 17.11.2007 № 781)

Пример. Выявленные нарушения

Проведена плановая выездная проверка МУП «Расчетный центр» МО ГО «Сыктывкар» Выявлены следующие нарушения:

1. … при ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию…
2. …при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.
3. … в случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные…
4. …если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных.

По результатам проверки выдано 4 предписания.

Еще примеры

…несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации;

…несоблюдение оператором установленных требований обработки персональных данных после достижения цели обработки.

…не соответствуют требованиям законодательства полученные с работников согласия на обработку персональных данных, не все сотрудники ознакомлены с Положением об особенностях обработки персональных данных в Департаменте, не соблюдаются требования по хранению материалов с персональными данными

«Гостиница …» осуществляет обработку персональных данных (сбор ксерокопии паспортных данных), избыточных по отношению к целям, заявленным при сборе персональных данных

Пример. Библитотека в Свердловске

10.11.2010

В ходе проверки установлено:

персональные данные сотрудников… обрабатываются в соответствии с положением о защите персональных данных работников.

Материальные носители хранятся в сейфе, в изолированном помещении, доступ к персональным данным имеют ограниченный круг субъектов.

На основании положения о защите персональных данных работников были получены обязательства о соблюдении режима конфиденциальности персональных данных.

В случае принятия новых работников на должности, указанные в положении, издаются приказы о допуске работников к обработке персональных данных.

Персональные данные пользователей обрабатываются в соответствии с положением по обеспечению безопасности персональных данных пользователей.

Оператор выполнил все требования законодательства в области персональных данных и получил высокую оценку своей работы.

Техническая защита ПДн

Технические мероприятия реализуются в рамках подсистем:

- управление доступом
- регистрация и учет
- обеспечение целостности
- антивирусная защита
- межсетевое экранирование
- обнаружение вторжений
- криптографическая защита

ВАЖНО:

Все используемые средства защиты информации должны пройти в установленном порядке процедуру оценки соответствия в ФСТЭК России.

Информационная безопасность офиса

Защита от вирусов	Предотвращение вирусных эпидемий и минимизация ущерба от вредоносного кода за счет централизации управления и модернизации существующей антивирусной системы.
Управление доступом	Разграничение доступа к информационным ресурсам, ограничение несанкционированного доступа, обеспечение безопасности данных.
Защита от утечек данных	Защита корпоративной информации от случайных и/или злонамеренных действий сотрудников, снижение коммерческих и репутационных рисков.
Виртуализация	Эффективное использование имеющихся ресурсов, повышение доступности бизнес-данных и приложений, снижение эксплуатационных затрат.
Резервное копирование	Поддержка непрерывности бизнес-процессов и обеспечение гарантированного срока восстановления данных.

АНТИВИРУСНЫЙ ЦЕНТР

Как обеспечить соответствие

АНТИВИРУСНЫЙ ЦЕНТР

Всего 4 шага…

- **Уведомить** уполномоченный орган о намерении осуществлять обработку персональных данных
- **Разработать** комплект документов, регламентирующих обработку персональных данных в организации
- **Внедрить** технические средства защиты персональных данных
- **Поддерживать** соответствие требованиям безопасности

АНТИВИРУСНЫЙ ЦЕНТР

Варианты сотрудничества

1. **Обследование, рекомендации, план действий;**

   Примерная продолжительность: 1-2 недели

2. **Обследование, разработка концепции обеспечения соответствия, разработка внешних и внутренних документов (включая Модель угроз и ТЗ)**

   Примерная продолжительность: 4-6 недель

3. **Проект «под ключ»**

   Примерная продолжительность: 8-12 недель

4. **Аудит на соответствие требованиям законодательства в области защиты ПДн**

   Примерная продолжительность: 1-2 недели

5. **Поддержание соответствия**

   Примерная периодичность: ежеквартально

Вариант 1 Обследование

Работы:

1. Выявление процессов обработки персональных данных.
2. Выявление информационных ресурсов, содержащих персональные данные.
3. Определение технических и эксплуатационных характеристик информационных систем персональных данных.
4. Определение имеющихся мер и средств защиты информации в информационной системе персональных данных.
5. Выявление существующей в организации базы организационно-распорядительной документации.

Результат:

1. Отчет об обследовании объекта защиты ПДн.
2. Экспертное заключение, содержащее экспертную оценку степени соответствия требованиям законодательства
3. Рекомендации по достижению соответствия требованиям.
4. План действий по достижению соответствия

Вариант 2 Орг. мероприятия

Работы:

- проведение классификации информационных систем ПДн;
- разработка внешних документов в области защиты ПДн (уведомление, договора, формы получения согласия и т.п.);
- разработка частной модели угроз безопасности ПДн при их обработке в информационной системе ПДн;
- разработка внутренних нормативно-регламентных документов по защите ПДн (положения, регламенты, акты, приказы, инструкции, журналы, планы);
- разработка технического задания на создание системы защиты ПДн;

Результат:

Подготовка полного комплекта документов в соответствии с требованиями Роскомнадзор в части организации процесса обработки персональных данных

Вариант 3 Проект «Под ключ»

Работы:

- разработка технического проекта;
- разработка рабочей документации по системе защиты ПДн
- реализация проектных решений по СЗПДн (монтаж оборудования, установка программного обеспечения, настройка оборудования и программного обеспечения, пуско-наладочные работы);
- опытная эксплуатация СЗПДн;
- приемочные испытания и ввод в эксплуатацию СЗПДн;
- обучение лиц, использующих средства защиты информации, применяемые в СЗПДн, правилам работы с ними;
- проведение аттестации СЗПДн (по желанию Заказчика)

Результат:

Реализация полного комплекса организационных и технических мероприятий в соответствии с требованиями законодательства

Вариант 4 – Аудит соответствия

Работы:

Выявление процессов обработки персональных данных.

Оценка состояния ИТ-инфраструктуры

Оценка полноты и актуальности документации

Анализ существующих политик ИБ

Проверка текущего состояния средств и систем ИБ

Результат:

Оценка состояния системы по 5-балльной шкале

Рекомендации по приведению в соответсвие

Вариант 5 Поддержание соответствия

Несколько причин для заключения контракта на сопровождение:

- внеплановые проверки
- изменение законодательства (требований);
- внедрение/ликвидация бизнес-систем;
- возникновение новых угроз безопасности ПДн;
- модернизация технических средств обработки и защиты ПДн;

АНТИВИРУСНЫЙ ЦЕНТР

13.04.2010

Управление Роскомнадзора по Республике Коми провело внеплановую проверку в отношении оператора ПД, Муниципального учреждения здравоохранения «Центральная поликлиника г. Сыктывкара», в ходе проверки выявлено нарушение в части хранения материальных носителей, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

АНТИВИРУСНЫЙ ЦЕНТР

29.09.2010

Протокол составлен в отношении юридического лица Института биологии Коми научного центра Уральского отделения РАН, которое в нарушение части ч.7 ст. 22 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» не представило в уполномоченный орган … сведений об изменении информации, содержащейся в уведомлении об обработке персональных данных.

Протокол был составлен по результатам планового мероприятия…

АНТИВИРУСНЫЙ ЦЕНТР

Приглашаем Вас:

- Обсудить вопросы обеспечения требований по ПДн
- Оценить эффективность защиты организации
- Подобрать оптимальное решение
- Получить ответы на практические вопросы
- Принять участие в следующих мероприятиях

+7 (495) 921-4008 www.AntiVirusPro.com uslugi_d@antiviruspro.com

АНТИВИРУСНЫЙ ЦЕНТР

Спасибо за внимание !!!

Сергей Золотухин
Руководитель направления
Дистрибуции услуг
ООО «Антивирусный Центр»