Илья Олегович Ольшак

ДЛЯ ЧЕГО НЕОБХОДИМО ЗАЩИЩАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Муниципальное бюджетное общеобразовательное учреждение гимназия №8
Техник, учитель информатики
Г. Новороссийск

С тех пор, как обработка, хранение и передача данных стала осуществляться в информационно-коммуникационных системах возможности злоумышленников для несанкционированного доступа или других неправомерных действий с такой информацией многократно возросли.
Поэтому в последнее время защите персональных данных граждан уделяется все большее и большее внимание. Персональные данные в руках мошенников легко конвертируются в реальные деньги, и, следовательно, являются товаром на черном рынке. Но, даже если злоумышленник не преследует цели финансового обогащения и конфиденциальность данных не находится под угрозой, оператору персональных данных может быть нанесен немалый ущерб путем нарушения целостности данных или их доступности, например в целях возмездия недовольным сотрудником.

Становится очевидным, что принятие мер по защите - это необходимость каждого учреждения обрабатывающего персональные данные. Эта необходимость прописана Законом №152-ФЗ.

Защита персональных данных сводится к реализации организационных и технических мер направленных на нейтрализацию угроз безопасности, определенных оператором, как актуальных.

Инструментами реализации технических мер выступают специально разработанные технические (аппаратные и программные) средства и системы защиты информации, направленные на предотвращение неправомерного доступа к информации (персональным данным), её утечки, модификации и блокирования.

Среди наиболее распространенных технических средств можно выделить:

1) средства защиты информации от несанкционированного доступа, которые решают такие задачи, как:
   - идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- регистрация событий безопасности;
- обеспечение целостности информационной системы и персональных данных;

На российском рынке данные средства представлены такими продуктами, как "SecretNet", "Dallas Lock" и другими.

2) Антивирусные средства, препятствующие реализации выполнению угроз программно-математического воздействия или попросту говоря вирусов. В Российском (и не только) сегменте особым предпочтением пользуются продукты "Антивирус Касперского" и "Dr.Web".

3) Системы обнаружения (предотвращения) вторжений - программные или аппаратные средства, предназначенные для выявления фактов сетевых атак через Интернет или внутри локальной сети. Часто данные функции присутствуют в составе антивирусных средств.

4) Функцию защиты информационной системы, ее средств, систем связи и передачи данных берут на себя межсетевые экраны и средства криптографической защиты информации (шифровальные средства). Зачастую средства МЭ и СКЗИ объединяются в одном аппаратном средстве, в таком, как например, получивший широкое распространение в России VipNet Coordinator HW 100\1000.

5)Любая система защиты информации, в том числе защита персональных данных требует контроля (анализа) защищенности, для этих целей применяются сканеры безопасности, такие, как "X-Spider" или RedCheck. Сканеры безопасности осуществляют функции по предотвращению уязвимостей, вызванных ошибками в коде, неверными настройками параметров безопасности, слабостью парольной защиты, несанкционированной установкой программного и аппаратного обеспечения, несвоевременной установкой критичных обновлений, нарушением принятых политик безопасности и др.

Но насколько мощной не была бы техническая защита, насколько стойкими не были бы криптографические алгоритмы, самым слабым звеном в защите информации зачастую является конечный пользователь.

Методы социального инжиниринга направлены на психологию человека и

позволяют обходить технические средства защиты. Основаны они на использовании слабостей человеческого фактора и считаются очень разрушительным, к применению защиты информации. Итогом такого воздействия может явиться то, что пользователь лично отправит персональные данные злоумышленнику или даст ему доступ к базам данным, даже не поняв, что совершает неправомерные действия.

Единственным рубежом защиты для такого вида атак выступают организационные меры защиты информации. Организационные меры, в принципе, должны являться ядром любой системы защиты информации и заключаются в регламентировании всех процессов защиты информации и осведомленности пользователей.

Нет толку от антивирусного средства, если базы его сигнатур регулярно не обновляются, как и нет толку от пароля в стиле "12345", "qwerty", "pass123" или «q1w2e3r4t5».

Другими словами пользователь должен быть обучен работе со средствами защиты информации, для чего в учреждении разрабатываются инструкции по антивирусной защите, по парольной защите, по обращению со средствами криптографической защиты информации и электронной подписи и любыми другими, применяемыми средствам защиты.

Так же пользователь должен знать, какая информация подлежит защите, для чего создаются перечни персональных данных, перечни мест хранения персональных данных, регламентируются права доступа сотрудников к персональным данным.

Пользователь должен осознавать свою ответственность за разглашение персональных данных, а посему должен быть ознакомлен с нормативной базой по защите информации, в том числе персональных данных.

В рамках нашей образовательной организации были разработаны и утверждены следующие документы, регламентирующие обработку и защиту персональных данных учащихся, родителей и сотрудников:

-приказ об организации работ по защите информации, содержащей персональные данные
-приказ об утверждении Регламентов по защите персональных данных
-регламент работы сотрудников МБОУ гимназия №8 с персональными данными
-инструкция по организации парольной защиты

-инструкция администратора систем информационной безопасности
-инструкция пользователя информационной системы персональных данных

В соответствии с этими документами предпринят ряд технических мер по повышению уровня информационной безопасности таких как:
-ограничение доступа к сети Интернет путём составления белых списков сайтов
-запрет на установку ПО для всех пользователей без каких-либо исключений
-доступ к ресурсам рабочих мест сотрудников обеспечивается только после ввода пароля пользователя
-на всех устройствах установлено и регулярно обновляется антивирусное ПО
-регулярно производится техническая инвентаризация парка компьютеров, на предмет установки постороннего ПО и оборудования.
-в связи с переводом 90% обрабатываемых ПД в АИС «Сетевой город. Образование» все сотрудники были проинформированы о недопустимости сохранения пароля в браузере, или его незамедлительной смены в случае возможного компрометирования.

Только выполнение технических и организационных мер может максимально снизить риск утечки персональных данных и сделать систему защиты информации эффективной.

Список использованной литературы

1. Шубинский М. И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных: учебное пособие. – СПб: НИУ ИТМО, 2013. –77 с

Источник: http://window.edu.ru/resource/416/80416/files/itmo1367.pdf#3

2.Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК от 18.02.2013 г. N 21)

Источник: http://pro-spo.ru/personal-data-security/4043-sostav-i-soderzhanie-organizaczionnyx-i-texnicheskix-mer-po-obespecheniyu-bezopasnosti-personalnyx-dannyx-pri-ix-obrabotke-v-informaczionnyx-sistemax-personalnyx-dannyx

3.Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"

Источник: http://www.consultant.ru/document/cons_doc_LAW_61801/

olshak@ya.ru