УДК 342.951 Вестник УрФО № 4(22) / 2016, с. 31–34

Васильева А. А., Сутягин С. А., Полякова Е. Н., Москвин В. В.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН ПРИ ПОДАЧЕ ЭЛЕКТРОННЫХ ОБРАЩЕНИЙ В ГОСУДАРСТВЕННЫЕ ОРГАНЫ

В статье рассмотрены проблемы обеспечения информационной безопасности персональных данных граждан РФ и пути их решения с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[1].

В теории защита персональных данных (далее – ПДн) кажется довольно простой, но, как показывает практика, имеется множество проблем. Во-первых, передача данных, содержащих ПДн граждан, по незащищенным каналам, в связи с эти возникает возможность их перехвата злоумышленниками. Во-вторых, отсутствие криптографической защиты обращений. В-третьих, проблема аутентификации отправителя и т.д.

Ключевые слова: *Информационная безопасность, электронные обращения, федеральный закон, государственные органы.*

Vasilyeva A. A., Sutyagin S. A., Polyakova E. N., Moskvin V. V.

THE PROBLEMS OF INFORMATION SECURITY OF CITIZENS' PERSONAL DATA WHEN SUBMITTING ELECTRONIC APPLICATIONS TO THE STATE DEPARTMENTS

The problems of information security of personal data of citizens of Russia and ways to decide it into account the Federal law of 27.07.2006 № 152-FZ «On personal data».

The theory of personal data protection seems rather simple, but in practice, there are many problems. Firstly, data containing citizens' personal data over unprotected channels, there is a possibility of interception by hackers. Secondly, there is no cryptographic protection of applications. Third, there is the sender's authentication problem.

Keywords: *Information security, electronic treatment, the federal law, the state departments.*

Введение

В целях повышения качества и эффективности отношений органов власти и общественности Государственной Думой был принят Федеральный закон от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»[2]. Он регламентирует один из способов взаимодействия государства и общества. В связи с этим у граждан РФ есть возможность отправлять обращения в госорганы, представленные в виде предложений, заявлений или жалоб.

К сожалению, в законодательстве имеются недоработки, которые ставят под угрозу обеспечение информационной безопасности персональных данных (далее - ПДн) граждан.

Цель работы – исследование проблемы обеспечения информационной безопасности персональных данных граждан при подаче электронных обращений в государственные органы РФ, а также разработка эффективного механизма их защиты.

Нами был сформулирован ряд задач:

1. Исследовать проблемы, связанные с безопасностью персональных данных и их передачи.

2. Выявить основные угрозы для информационной безопасности ПДн.

3. Разработать и предложить к реализации комплекс соответствующих мер защиты.

Подача обращений через региональный сайт МФЦ

Для граждан РФ существует два способа подачи электронного обращения: с помощью заполнения формы на сайте органа местного самоуправления или на сайтах многофункциональных центров (далее - МФЦ), целью которых является автоматизация предоставления услуг населению.

В случае, когда пользователю необходимо отправить обращение через сайт МФЦ, их принуждают согласиться с передачей личных данных в открытом виде следующим условием: «Я подтверждаю свое согласие на передачу информации в электронной форме обращения (в том числе персональных данных) по открытым каналам связи сети Интернет».

При отказе пользователя действие не будет произведено. Причем на некоторых сайтах вообще может и не быть никакой информации об условиях передачи, либо она может быть затеряна в большом количестве другой информации.

Поэтому можно сделать вывод, что организация подобным образом снимает с себя ответственность за хищение личных данных граждан.

На рисунке 1 приведена реальная схема механизма подачи, перенаправления и ответа на электронные обращения. На первом этапе ПДн граждан РФ не защищены. Отношения же МФЦ и госорганов в информационной среде регулируются СМЭВ (т.е. «Единой системой межведомственного электронного взаимодействия»). Но при отправке ответа пользователю снова возникает угроза хищения личных данных.

Также на территории России действует Единый портал «Госуслуги», который тоже предоставляет различные функции и имеющий большую популярность среди населения. К сожалению, на нем не реализована услуга по подаче электронных обращений, что могло бы обеспечить информационную безопасность ПДн на первом этапе, в связи с тем что используется https-соединение.

Экспериментальная часть

В качестве доказательства наличия угрозы хищения ПДн, на базе кафедры «Безопасность информационных и автоматизированных систем» Курганского государственного университета было проведено два эксперимента. В качестве примера был выбран сайт московского филиала Многофункционального центра и рассматривалась атака MITM

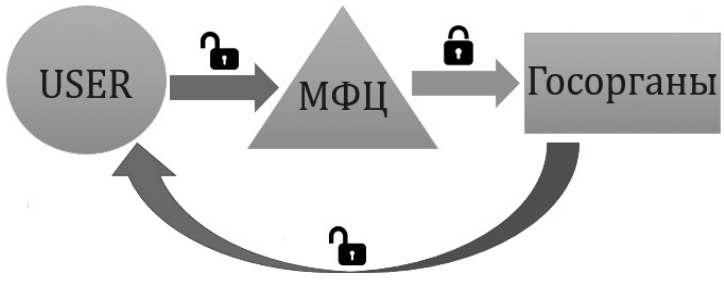

Рис. 1. Общая схема системы.

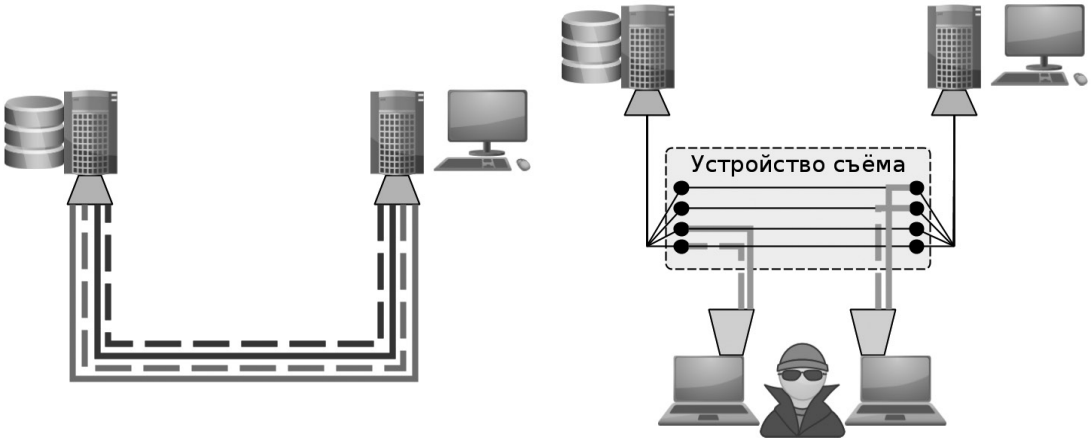

Рис. 2.
а) Общая схема работы кабеля 4-парного кабеля UTP категории 5е.
б) Принцип работы устройства съёма информации

(«Man in the middle») на узел пользователя, отправляющего свои данные через форму обращения на сайте.

В первом эксперименте использовалось специально подготовленное устройство (рис. 2), с помощью которого проводилась хакерская атака в условиях наличия прямого доступа к локальной сети атакуемого хоста. Во втором эксперименте съём информации производился непосредственно с кабеля с помощью двух контактных зажимов (рис. 3). В обоих случаях пакеты с информацией, введенной на форме, были перехвачены.

В ходе изучения данного вопроса обнаружили, что некоторые сайты, на которых предоставляется услуга формирования электронного обращения, например, сайты органов местного самоуправления, имеют аналогичную уязвимость.

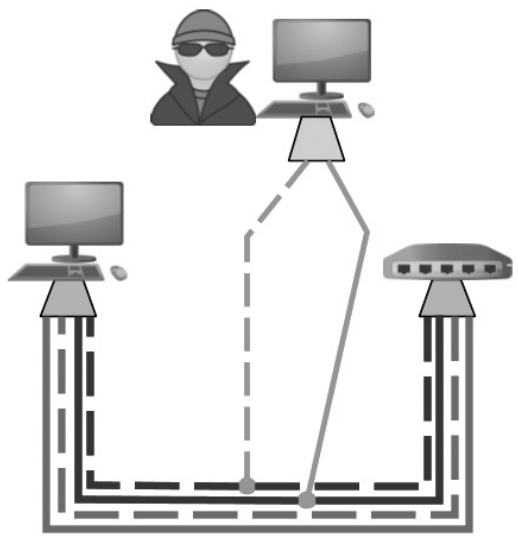

Рис. 3. Общая схема работы

Возникает проблема аутентификации личности отправителя и одним из способов решения данной проблемы это использование электронной цифровой подписи (далее ЭЦП). В связи с тем, что ЭЦП редко используется гражданами и имеется не у всех, ее стоимость довольно велика, то смысла ее приобретать для отправки всего одного обращения нет. Выходом из данной ситуации может быть наличие у МФЦ своей собственной электронной подписи, с помощью которой можно было бы бесплатно заверять документы граждан.

Для обеспечения равного доступа к рассматриваемой услуге, например, подача электронного обращения слабовидящими гражданами, должна существовать возможность формирования копии ответа для них шрифтом Брайля.

Заключение

Таким образом, в ходе исследования были выявлены проблемы, которые связаны не только с безопасностью передачи электронных обращений в госорганы, но и с другими аспектами.

Для обеспечения безопасности персональных данных, передаваемых по каналам сети Интернет, необходимо использовать:

- протоколы защиты VPN и TLS;
- программные и программно-аппаратные средства шифрования;
- средства электронной подписи.

Для проверки подлинности личных данных пользователя необходимо:

- отправлять обращения в виде электронного документа;
- использовать ЭЦП;
- заверять обращения с помощью собственной подписи МФЦ.

Для оптимизации эффективности МФЦ необходимо:

- создание общероссийской сети МФЦ;
- объединение всех центров на одном сайте с возможностью выбора региона;
- резервное копирование обращений и ответов на них для возможности получения ответа в другом регионе;
- организация региональных мобильных центров;
- добавить функцию формирования обращений на портале Госуслуги;
- рассылать SMS-уведомления о статусе обращений.

Примечания

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных».

2. Федеральный закон от 02.05.2006 N 59-ФЗ (ред. от 03.11.2015) «О порядке рассмотрения обращений граждан Российской Федерации».

ВАСИЛЬЕВА Алена Алексеевна, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: alena.alekseyevna@yandex.ru

СУТЯГИН Сергей Александрович, студент кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. Email: svd.sergey95@gmail.com

ПОЛЯКОВА Елена Николаевна, кандидат педагогических наук, заведующий кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: penelena1972@yandex.ru

МОСКВИН Владимир Викторович, старший преподаватель кафедры «Безопасность информационных и автоматизированных систем» технологического факультета ФГБОУ ВО «Курганский государственный университет». 640020, г. Курган, ул. Советская, д. 63, стр.4. E-mail: bias.kgsu.techno@gmail.com

VASILYEVA Alena Alekseyevna, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: alena.alekseyevna@yandex.ru

SUTYAGIN Sergey Alexandrovich, student of the Department of «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. Email: svd.sergey95@gmail.com

POLYAKOVA Elena Nikolayevna, the candidate of pedagogical Sciences, head of Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: penelena1972@yandex.ru

MOSKVIN Vladimir Viktorovich, senior teacher of the Department «Security of information and automated systems» of the faculty of technology of the «Kurgan state University». 640020, Kurgan, Sovetskaya street, 63, p. 4. E-mail: bias.kgsu.techno@gmail.com